Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

Е.В. Чернова

УПРАВЛЕНИЕ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

*Утверждено Редакционно-издательским советом университета
в качестве практикума*

Магнитогорск
2022

УДК 37:004

Рецензенты:

генеральный директор
ООО «Корпоративные системы Плюс»
Ю.А. Чудинова

заместитель директора,
ГБУ ДО «Дом юношеского технического творчества Челябинской области»,
руководитель ДТ «Кванториум»
Д.П. Полушкин

Чернова Е.В.
Управление непрерывностью бизнеса [Электронный ресурс] : практикум / Елена Владимировна Чернова ; ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». – Электрон. текстовые дан. (1,90 Мб). – Магнитогорск : ФГБОУ ВО «МГТУ им. Г.И. Носова», 2022. – 1 электрон. опт. диск (CD-R). – Систем. требования : IBM PC, любой, более 1 GHz ; 512 Мб RAM ; 10 Мб HDD ; MS Windows XP и выше ; Adobe Reader 8.0 и выше ; CD/DVD-ROM дисковод ; мышь. – Загл. с титул. экрана.

Практикум составлен в соответствии с типовой программой дисциплины «Управление непрерывностью бизнеса» для магистров направления 09.04.03 Прикладная информатика. Практикум содержит теоретический материал, необходимый для выполнения заданий практической работы, задания к практическим работам и примеры выполненных заданий, глоссарий, список использованных и рекомендованных источников для успешного освоения практических заданий в области управления непрерывностью бизнеса.

Сборник предназначен для студентов очной и заочной форм обучения направления 09.04.03 Прикладная информатика.

УДК 37:004

Содержание

ВВЕДЕНИЕ 4
Практическая работа 1. Характеристика организации 5
Пример выполнения практической работы 1 8
Практическая работа 2. Идентификация целей обеспечения непрерывности бизнеса 11
Пример выполнения практической работы 2 26
Практическая работа 3. Оценка воздействия на бизнес по методу BIA 28
Пример выполнения практической работы 3 33
Практическая работа 4. Ранжирование критически важных бизнес-процессов. 37
Пример выполнения практической работы 4 38
Практическая работа 5 Оценка угроз критическим видам деятельности организации 39
Пример выполнения практической работы 5 48
Практическая работа 6. Оценка воздействий и долговременных последствий отказов, отсутствия активов и ресурсов 49
Пример выполнения практической работы 6 52
Практическая работа 7. Стратегия управления непрерывностью бизнеса 53
Пример выполнения практической работы 7 55
Практическая работа 8 Разработка организационно-распорядительной документации 60
Пример выполнения практической работы 8 65
Практическая работа 9. Тестирование планов 69
ГЛОССАРИЙ 70
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 75

ВВЕДЕНИЕ

Цель изучения дисциплины «Управление непрерывностью бизнеса» – формирование компетенций специалистов в области разработки и реализации эффективного управления непрерывностью бизнеса в соответствии с требованиями стандартов BS 25999-1:2006 «Code of Practice», BS 25999-2:2006 «Specification» и ГОСТ Р 53647.3-2015 «Менеджмент непрерывности бизнеса».

Данный практикум направлен на формирование следующих компетенций:

ПК-3 – способностью ставить и решать прикладные задачи в условиях неопределенности и определять методы и средства их эффективного решения

Знать: возможности применения методов управления непрерывностью бизнеса в условиях неопределенности.

Уметь: выявлять угрозы непрерывности бизнеса предприятия в условиях неопределенности и находить способы их предотвращения или снижения.

Владеть: навыками использования программных средств для поддержки управления непрерывностью бизнеса.

ПК-12 – способностью проектировать архитектуру и сервисы ИС предприятий и организаций в прикладной области.

Знать: особенности проектирования архитектуры и сервисов ИС предприятия с точки зрения обеспечения непрерывности бизнеса.

Уметь: определять критически важные элементы архитектуры и сервисов ИС предприятия и обеспечивать минимизацию рисков нарушения непрерывности бизнеса.

Владеть: систематизированными знаниями в области обеспечения информационной безопасности и защиты информации при проектировании архитектуры и сервисов ИС предприятия в области экономики и управления.

ПК-14 – способностью принимать эффективные проектные решения в условиях неопределенности и риска

Знать: методы управления непрерывностью бизнеса в условиях риска и неопределенности.

Уметь: определять требования и мероприятия по обеспечению непрерывности бизнеса и внедрять управление непрерывностью бизнеса в культуру организации.

Владеть: навыками принятия эффективных решений при управлении непрерывностью бизнеса в условиях неопределенности и риска.

В практикуме приведены выполненные практические работы на примере вымышленной организации.

Практическая работа 1.
Характеристика организации

Задание 1.

Технико-экономическая характеристика организации. Цели и задачи деятельности. Стратегия развития.

Основные технико-экономические показатели предприятия – это система измерителей, абсолютных и относительных показателей, которая характеризует хозяйственно-экономическую деятельность предприятия. Комплексный характер системы технико-экономических показателей позволяет адекватно оценить деятельность отдельного предприятия и сопоставить его результаты в динамике.

Цель организации представляет собой конечное состояние или желаемый результат, к которому стремится любая компания. Компания имеет всегда одну общую цель, к достижению которой должны стремиться все участники трудового коллектива.

Задачи организации представляют собой цели, достижение которых необходимо к определённому времени в пределах периодов, на которых рассчитывается управленческое решение. Задачи организации являются целями, которые не привязаны ко времени.

Цели и задачи организации могут включать в себя завоевание и удержание доли определенного рынка, достижение более высокого качества продукции, повышение прибыльности компании, достижение максимального уровня занятости и др. Они задают общий ориентир для деятельности и могут определяться интересами владельцев, ситуацией внутри компании и внешней средой, а также размером капитала компании. Их могут ставить как владельцы компании, так и руководящие работники и персонал. Владельцы при формулировании и постановке цели и задач организации опираются на собственные приоритеты, чаще всего это получение прибыли за счет производства или продаж.

Главной целью большинства предприятий является превышения результата над понесенными затратами, то есть получение максимальной прибыли и высокого уровня рентабельности. Для достижения данной цели предприятиями выполняется ряд задач: выпуск высококачественной продукции, внедрение новых технологий, разработка стратегии и тактики поведения, обеспечение конкурентоспособности, забота о работниках и др.

Стратегическая установка, или миссия, организации может быть осмыслена как причина ее существования, как главная и долгосрочная цель деятельности организации. Любая организация имеет стратегическую установку, или миссию, даже если она не представлена в явном виде и основатель организации никогда не ставил перед собой цель ее сформулировать. Миссия организации – это одна из наиболее важных отличительных черт данной организации от множества ей подобных, действующих рядом, в одной и той же отрасли.

Миссия организации, в сущности, означает попытку ответить на вопрос, в чем состоит конечный смысл деятельности организации. Она обычно довольно широка по масштабу и зачастую выглядит как описание долгосрочных пер-

спектив организации. Разумеется, нет серьезных оснований искать миссию существования небольших коммерческих организаций – парикмахерских, мастерских по ремонту бытовой техники, магазинов продовольственных товаров и им подобных. Для них и им подобных долгосрочная перспектива, как правило, состоит в выживании в жесткой конкурентной среде и, по возможности, укреплении и расширении бизнеса. Так же трудно определять миссию для организаций, деятельность которых строго регламентирована сверху, например, органов муниципального управления. Однако в случае корпораций, крупных организаций бизнеса проблема определения миссии может становиться одной из сложнейших проблем стратегического развития.

Согласно Ф. Дэвиду, стратегическая установка должна отражать следующие вопросы [7]:

1. Покупатели. Указывается, кто является покупателями организации.
2. Продукция или услуги. Описание основных видов продукции и услуг организации.
3. Рынки. Формулируется сфера конкуренции фирмы.
4. Технология. Сообщается о том, является ли технология предметом внимания организации.
5. Формулирование широких экономических задач фирмы.
6. Философия. Подтверждение основных убеждений, ценностей и философских приоритетов организации.
7. Самооценка. Формулирование недостатков организации и ее конкурентных преимуществ.
8. Забота об имидже. Формулирование того, как организация хотела бы выглядеть в глазах общественности.
9. Отношение к персоналу. Заявление об отношении компании к ее персоналу.

Связь между миссией, целями и задачами организации показана на рис. 1 [7].

Рис. 1. Соотношение между миссией, целями и задачами организации

Стратегия развития организации – «план работы всех подразделений на ближайший год или несколько лет» [18]. Во время разработки закладываются ожидаемые результаты и расчеты. Формирование этой подробной бумаги играет важную роль – помогает адаптироваться в условиях быстро меняющейся бизнес-среды.

Чего обязательно коснется документ:

– миссии;
– основного направления;
– инструментов, с помощью которых будут достигаться цели;
– как позиционирует себя фирма с внутренней и внешней стороны;
– порядка действий, которые нужно выполнить, если на организацию повлияют изнутри или извне;
– социальной стороны жизни.

Этот план рассчитывает, каким путем будет быстрее и эффективнее достигать поставленные задачи.

Задание 2.

Обязательства перед партнерами и контрагентами.

Партнер – участник совместной с организацией связи деятельности по предоставлению услуг клиентам, связанный с организацией договорными отношениями, которые определяют долю прибыли и материальную ответственность по рискам

Контрагент – физическое или юридическое лицо, учреждение или организация, являющееся стороной в гражданско-правовых отношениях, при заключении договора. Контрагентом по отношению друг к другу является каждая из сторон. Каждый из партнеров, подписавших договор, является контрагентом. Контрагенты связаны теми или иными обязательствами согласно подписанному договору.

Обязательства перед другими лицами включают в себя информацию о том, какие факторы могут привести к нарушению обязательства перед партнером или контрагентом.

Пример выполнения практической работы 1

Задание 1. Технико-экономическая характеристика организации. Цели и задачи деятельности. Стратегия развития.

Цель организации ЗАО «ПромАвтоматика» – разработать и внедрить комплексные системы автоматизации для предприятий металлургии, энергетики, горнодобывающей промышленности и др.

Задачи:

Обследование объекта автоматизации

Сбор, систематизация и анализ функциональных требований Заказчика, общий анализ предприятия, технологии и особенностей производства, оценка технического состояния, определение текущего уровня автоматизации, разработка технико-коммерческих предложений или технико-экономических обоснований

Разработка Технического задания

Грамотное и квалифицированное составление технических заданий согласно ГОСТ и в тесном сотрудничестве со специалистами заказчика на основании результатов обследования объекта автоматизации, согласование и утверждение его заказчиком

Проектирование

Разработка проектных решений в полном соответствии с ГОСТ: технических проектов, рабочей документации или технорабочих проектов. Подготовленная нами проектная документация реально используется Заказчиком на всех стадиях внедрения и эксплуатации проекта

Поставка оборудования и ПО

Подбор и поставка любых технических и программных средств от ведущих мировых производителей для построения систем автоматизации и информационной структуры предприятия

Программирование

Программирование контроллеров, разработка локальных SCADA-систем (АСУ ТП), интегрированных систем диспетчерского контроля различного масштаба, систем управления цеховым энергоснабжением, автоматизированных систем управления производством (АСУ П) и многое другое

Монтаж, шеф-монтаж

Сборка и монтаж материалов и оборудования на объекте собственными силами или с привлечением субподрядных организаций, а также оказание консультационных услуг персоналу заказчика или сторонним организациям во время проведения монтажных работ по проектам компании

Пусконаладочные работы

Сборка и монтаж материалов и оборудования на объекте собственными силами или с привлечением субподрядных организаций. Проведение пусконаладочных работ по собственным проектам уровня АСУ ТП, АСУ П (MES), проектам сетевой инфраструктуры, а также управление пусконаладкой сторонних организаций. Компания имеет практический опыт работ как генподрядчик по запуску систем в эксплуатацию

Обучение

Организация обучения персонала предприятий, на которых внедряются системы автоматизации, разработанные компанией

Техническая поддержка

Гарантийное обслуживание внедренных систем автоматизации, сетей и систем связи, постгарантийное обслуживание по сервисным договорам, ремонт оборудования

Лаборатория неразрушающего контроля

Диагностика любых объектов строительства, промышленности и электроэнергетики, в работе которых присутствует теплообмен: наружных и внутренних поверхностей строительных объектов, генераторов, воздушных линий электропередач, кабелей и их соединений, трансформаторов, дымовых труб, трубопроводов, тепловых и котельных станций и др.

Задание 2. Обязательства перед партнерами и контрагентами

11 апреля в г. Магнитогорске состоялось подписание официального соглашения о партнерстве между компаниями B&R Automation и ЗАО «ПромАвтоматика».

Начиная с апреля текущего года компания B&R Automation является партнером ЗАО «ПромАвтоматика» в реализации проектов в области автоматизации технологических процессов в Уральском регионе. Сотрудничество заключается в совместном предложении комплексных решений по автоматизации технологических процессов и оборудования для различных отраслей промышленности. Широкий спектр продукции, производимой компанией B&R, включающий в себя программируемые логические контроллеры, панели оператора, промышленные компьютеры, регулируемый электропривод, а также программно-технические системы управления для комплексной автоматизации производства существенно расширяет возможности ЗАО «ПромАвтоматика» в стремлении оказывать максимально качественную поддержку предприятиям региона.

Специалисты ЗАО «ПромАвтоматика» прошли полный цикл обучения и сертифицированы для работы с продукцией B&R.

B&R – частная компания со штаб-квартирой в Австрии и офисами во всем мире. Как глобальный лидер в автоматизации производства, B&R объединяет современные технологии с новаторскими разработками, предлагая законченные решения для автоматизации машин и технологических процессов, управления движением, визуализации, промышленной связи и обеспечения безопасности клиентам в различных отраслях промышленности. С промышленными стандартами связи (POWERLINK и openSAFETY) и мощной программной средой разработки Automation Studio компания B&R делает настоящим будущее промышленной автоматизации. Инновационный дух, позволяющий B&R держаться на передовой промышленной автоматизации, позволяет упрощать процессы и превосходить ожидания заказчика.

За более чем 17 лет своей деятельности компанией реализовано более 570 проектов различного масштаба и степени сложности в таких отраслях как металлургия, горнорудная промышленность, энергетика, телекоммуникации, государственное управление.

У компании имеются давние налаженные связи со смежными специализированными организациями города, что значительно облегчает процесс проектирования и выполнения ряда смежных работ. Работа ведется в тесном сотрудничестве с ведущими проектным институтом и строительно-монтажным предприятием на Южном Урале – ОАО «МАГНИТОГОРСКИЙ ГИПРОМЕЗ», ОАО «ПРОКАТМОНТАЖ».

Практическая работа 2.
Идентификация целей обеспечения непрерывности бизнеса

Задание 1

Описать основные бизнес-процессы и активы организации.

Бизнес-процесс – совокупность взаимосвязанных мероприятий или работ, нацеленных на создание конкретного товара или услуги для потребителей. Проще говоря, это любая логическая последовательность действий, которая стабильно зациклена и приводит к определенной конечной цели, поставленной перед компанией. Важно уточнить, что коммерческая составляющая не является обязательным элементом в этом вопросе. К примеру, процессы контакта между сотрудниками внутри предприятия (отпуск, перевод, увольнение и т.д.) также могут относиться к бизнес-процессам.

Бизнес-процесс – логическая последовательность человеческих действий (или группы лиц) в рабочем коллективе. Целью его описания является анализ и регламентация определенных событий в штате работников.

Процесс определения бизнес-процессов в деятельности юридического лица и выделения среди них критичных предполагает проведение анализа всех управленческих, технологических, производственных, финансово-экономических и иных бизнес-процессов юридического лица [3]. Процесс включает следующие процедуры (рис. 2):

– составление перечня всех управленческих, технологических, производственных, финансово-экономических и иных бизнес-процессов в деятельности юридического лица;

– высокоуровневую оценку негативных последствий от нарушения бизнес-процессов в деятельности юридического лица по каждому критерию, определенному постановлением Правительства РФ от 08.02.2018 г. № 127;

– формирование перечня критичных бизнес-процессов в деятельности юридического лица.

При составлении Перечня бизнес-процессов надо учитывать, что [3]:

– под управленческими бизнес-процессами понимаются любые процессы в деятельности юридического лица, направленные на управление выполнением функций (полномочий) или осуществления видов деятельности юридическим лицом. Управленческие бизнес-процессы представляют собой совокупность циклических действий, связанных с выявлением проблем, поиском и организацией выполнения принятых решений для управляемых объектов;

– под технологическими бизнес-процессами понимаются любые процессы в деятельности юридического лица, которые обслуживают основные бизнес-процессы, направленные на выполнение функций (полномочий) или осуществление видов деятельности юридическим лицом;

– под производственными бизнес-процессами понимаются любые процессы в деятельности юридического лица, направленные на достижение конечного результата выполняемых функций (полномочий) или видов деятельности юри-

дического лица. Производственные процессы являются линейными процессами на выходе которых предполагается определенный результат;

– под финансово-экономическими бизнес-процессами понимаются любые процессы в деятельности юридического лица, связанные с экономическими, финансово-денежными, учетными, фискальными аспектами деятельности юридического лица, а также с обеспечением текущей деятельности юридического лица посредством реализации финансовых прав и исполнения финансовых обязательств.

Рис. 2. Состав и содержание процесса определения бизнес-процессов юридического лица

Модель входов-выходов предполагает, что любую деятельность организации можно описать как преобразование входов в выходы. Это справедливо как для отдельного бизнес-процесса, так и для деятельности всей организации.

При этом входы процесса удобно классифицировать на преобразующие, преобразуемые и управляющие. На рисунке 3 изображены входы и выходы процесса, расположенные согласно методологии SADT и нотации IDEF0 [6].

Рис. 3. Модель процесса, отражающая входы и выходы с их классификацией

Взяв за признак классификации выходы бизнес-процессов, можно разделить их по 4 группам (см. рис. 4 и табл. 1) [6]:

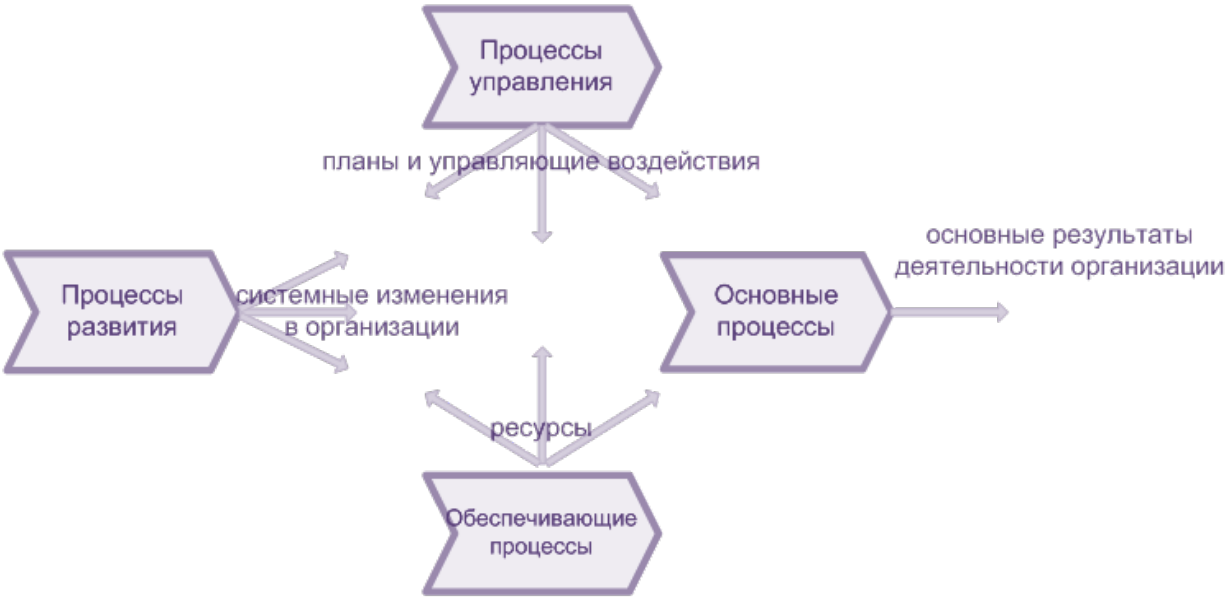

Рис. 4. Четыре группы бизнес-процессов любой организации

Таблица 1

Назначение и результаты бизнес-процессов

Тип бизнес-процесса	Назначение процесса	Основной результат (выход) процесса
Основной	Создание ценности для потребителей организации	Ценность для потребителя (окончательная или промежуточная)
Обеспечивающий	Обеспечение ресурсами остальных процессов	Ресурсы для всех других видов процессов
Управленческий	Управление организацией	Планы и управляющие воздействия для всех других видов процессов
Развития	Развитие организации или отдельных подсистем в ней	Изменения в организации (изменения в инфраструктуре, новые методы взаимодействия внутри организации и т. п.).

При этом взаимосвязь первых трёх групп процессов можно представить следующим образом.

Основные процессы для функционирования требуют ресурсы, которые поступают либо из внешней среды, либо от обеспечивающих процессов (рис. 5) [6].

Управленческие процессы связаны с основными в единый контур управления. Деятельность в организации планируется (формально или неформально). Соответствующие планы – это выход управленческого процесса, связанного с планированием, и управляющий вход управленческого процесса, связанного с регулированием (корректировкой) деятельности (см. рис. 6). Основная деятельность организации порождает информационные потоки, которые обычно обрабатываются обеспечивающим процессом, формирующим отчётность для управленческих процессов. Управленческий процесс регулирования оценивает ситуацию и при необходимости формирует управленческие воздействия на основные процессы [6].

Рис. 5. Взаимосвязь основных и обеспечивающих процессов

Рис. 6. Взаимосвязь основных и управленческих процессов в контуре управления

Последовательное выделение процессов, начиная с их результатов

Вышеописанные связи процессов позволяют выделять процессы один за другим, отталкиваясь от результатов деятельности всей организации.

Различные подходы к выделению и описанию бизнес-процессов

Первым шагом любой из перечисленных методологий является выделение бизнес-процессов, определение их четких границ и назначение владельцев. Менеджеры, получившие образование в разных местах и имеющие различный опыт, понимают термин «бизнес-процесс», выделяют и описывают процессы по-своему.

Рассмотрим три основных подходах к определению границ бизнес-процессов, которые часто являются причиной основных разногласий среди менеджеров, хотя и это деление достаточно условно. Итак, процесс – это последовательность действий, сгруппированных [19]:

– по виду деятельности (схожие функции);
– по результату деятельности (продукту);
– по добавленной ценности для клиента.

Первый подход ориентирован на описание последовательности действий, производимых работниками для достижения результата в рамках своего функционального подразделения; второй позволяет сгруппировать работы по принципу выделения заказчика и продукта для него; третий выделяет и рассматривает процессы как совокупность действий, добавляющих ценность для клиента. Рассмотрим области применения, достоинства и недостатки каждого подхода [19].

Первый подход часто применяется при работе над различными проектами автоматизации. При этом делаются «фотографии» существующих и будущих операций на предприятии, зачастую даже без построения моделей верхнего уровня, а если они и строятся, то скорее напоминают функциональную иерар-

хию. Такой подход вполне приемлем для привязки IT-решений к реально действующему предприятию, позволяет на этапе проектирования продемонстрировать заказчику предполагаемые результаты деятельности и вполне адекватно проводить работы по постановке IT-решений и внедрению программного обеспечения.

На рис. 7 показана модель OBM (Oracle Business Model), отображающая такой подход [19]. Модели этого типа отличаются существенным недостатком – предприятие описывается в терминах функциональной деятельности. Поэтому при декомпозиции модели бизнес-процессы и операции описываются как деятельность, распределенная по различным функциональным подразделениям и специалистам, что нарушает главный принцип реинжиниринга – «один процесс – одно подразделение – один бюджет – один владелец процесса». Именно этот принцип (принцип процессного управления) ставили во главу угла М. Хаммер, Дж. Чампи и другие гуру в области реинжиниринга и процессного подхода.

Второй подход основан на выделении процессов по результатам деятельности (а не по предмету, как в предыдущей модели). Наиболее известными моделями, использующими данный подход, являются тринадцати- и восьмипроцессные универсальные модели, а также модель Шеера, их особенность заключается в четком агрегировании работ «по результату». Если при внедрении процессного управления владельцу процесса административно подчиняются все участники процесса, такие модели позволяют разрабатывать и внедрять «плоские» структуры. Такие структуры предъявляют крайне жесткие требования к квалификации исполнителей, плохо понимаются линейными управленцами (заказчиками) и крайне сложны в разработке – в силу высокой абстрагированности принципов и понятий, применяемых при моделировании. В то же время эти структуры, в случае их внедрения, позволяют существенно сокращать численность персонала, в действительности оптимизировать деятельность предприятия, придавать «прозрачность» и управляемость бизнесу. При применении данного подхода следует иметь в виду, что поскольку понятие «результат» само по себе не является однозначным, данный подход предполагает множество вариаций на тему. Самая большая опасность при применении данного подхода кроется в определении результата, поскольку каждую функцию можно представить как отдельный процесс, в результате которого что-либо производится, а затем объединить полученные «процессы» в уже известную модель «по предмету», тем самым нивелируя все преимущества данного подхода.

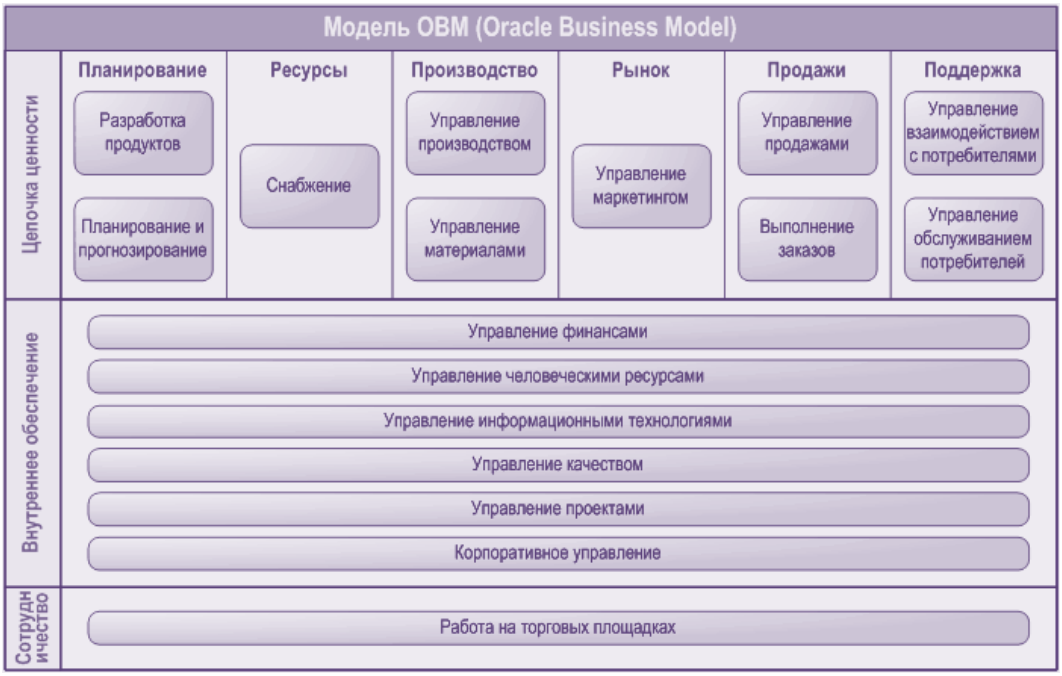

Рис. 7. Oracle Business Model

Тринадцатипроцессная модель. Технический отчет ИСО и МЭК (ИСО/МЭК/ТО 15504), классифицируя процессы, как следствие классифицирует и результаты этих процессов (табл. 2) [19]. Согласно ИСО/МЭК/ТО 15504, все процессы делятся на следующие категории:

– «потребитель – поставщик» – процессы непосредственно затрагивающие потребителя, поддерживающие разработку и передачу продукта потребителю и обеспечивающие правильные эксплуатацию и использование продукта;

– инженерные – процессы, непосредственно специфицирующие, реализующие и сопровождающие продукт;

– вспомогательные – процессы, результаты которых могут быть использованы в любых других процессах (включая и другие вспомогательные процессы) на различных этапах жизненного цикла продукта;

– управленческие – процессы, содержащие общие действия, которые могут быть использованы теми, кто управляет проектом любого типа или процессом в рамках жизненного цикла продукта;

– организационные – процессы определения бизнес-целей организации и разработки процессов, продуктов или развития активов.

Таблица 2

Тринадцатипроцессная модель

Название бизнес-процесса	Описание бизнес-процесса	Результат бизнес-процесса
Изучение рынков и потребителей	Определение нужд и желаний потребителей Измерение удовлетворенности потребителей Мониторинг изменений рынка и/или ожиданий потребителей	Запросы на создание продуктов, удовлетворяющих новые потребности потребителей

Продолжение табл. 2

Название бизнес-процесса	Описание бизнес-процесса	Результат бизнес-процесса
Разработка видения и стратегии	Мониторинг внешней среды Разработка концепции и стратегии бизнеса Разработка структуры организации и взаимосвязей между структурными единицами Формулирование и принятие целей организации	Стратегия организации
Разработка продуктов и услуг	Разработка концепций новых продуктов/услуг и планов Проектирование, создание и тестирование прототипов продуктов/услуг Внесение улучшений в существующие продукты/услуги Тестирование эффективности новых или усовершенствованных продуктов/услуг Подготовка к производству Управление процессом разработки продуктов/услуг	Техническая документация и порядки, необходимые для производства товаров и услуг
Маркетинг и продажи	Разработка стратегии маркетинга и продаж продуктов/услуг Продажа продуктов/услуг Управление заказами потребителей	Заказы потребителей
Производство и поставка продуктов и услуг (производственные компании)	Планирование и приобретение необходимых ресурсов Преобразование ресурсов и необходимых компонентов в продукты Транспортировка и доставка материалов и продуктов Управление процессом поставки и его выполнение	Выполненные заказы потребителей
Производство и поставка продуктов и услуг для организаций, ориентированных на предоставление услуг	Планирование и приобретение необходимых ресурсов Повышение квалификации персонала Предоставление услуги потребителям Обеспечение качества услуги	Выполненные заказы потребителей
Выставление потребителям платежных требований и сервис	Выставление платежных требований Предоставление послепродажного сервиса Ответы на запросы потребителей	Деньги
Профессиональное и карьерное развитие кадров и управление кадрами	Создание стратегии работы с персоналом Доведение (декомпозиция) стратегии до уровня рабочих мест Управление расстановкой персонала Развитие и обучение сотрудников Управление производительностью сотрудников, развитие системы вознаграждения и признания их заслуг Обеспечение комфортного самочувствия и удовлетворенности сотрудников Обеспечение вовлеченности персонала Управление отношениями между менеджерами	Персонал, мотивированный на достижение стратегических целей компании

Окончание табл. 2

Название бизнес-процесса	Описание бизнес-процесса	Результат бизнес-процесса
	и сотрудниками Разработка информационной кадровой системы	
Управление информационными ресурсами и технологиями	Планирование управления информационными ресурсами Разработка и развертывание корпоративных систем поддержки Реализация системы безопасности и средств контроля безопасности Управление хранением и выборкой информации Управление функционированием инфраструктуры здания (освещением, отоплением, вентиляцией и др.) и локальной сетью Управление информационным обслуживанием Обеспечение возможности коллективного доступа к информации и создание информационных центров Оценка и аудит качества информации	Инфраструктура, готовая для использования внутри компании
Управление финансовыми и материальными ресурсами	Управление финансовыми ресурсами Обработка финансовых и бухгалтерских транзакций Отчетная информация Проведение внутреннего аудита Управление функцией расчета налогов Управление материальными ресурсами	Возможность и право компании продолжать бизнес
Исполнение программы управления охраной внешней среды	Формулировка стратегии управления охраной внешней среды Обеспечение соблюдения законодательства на эту тему Повышение квалификации и обучение сотрудников Реализация программы предотвращения загрязнения внешней среды Управление мероприятиями по снижению опасности загрязнения Реализация программы реагирования на чрезвычайные ситуации Управление отношениями с государственными органами по охране внешней среды и со СМИ	Возможность компании продолжать бизнес
Управление внешними связями	Взаимодействие с акционерами Управление взаимодействием с государственными органами Выстраивание отношений с арендодателем Разработка программы связи с общественностью Взаимодействие с Советом директоров Выстраивание отношений с местной общиной Управление юридическими и этическими вопросами	Положительный имидж компании
Управление улучше-	Измерение производительности организации	Конкурентоспособ-

Название бизнес-процесса	Описание бизнес-процесса	Результат бизнес-процесса
ниями и изменениями	Проведение оценки качества Проведение сопоставительного анализа (бенчмаркинга) производительности Улучшение процессов и систем Реализация всеобщего управления на основе качества (TQM)	ность компании на рынке

Данные категории могут быть сгруппированы по трем основным типам [19]:

– основные процессы – «потребитель – поставщик», инженерные;
– вспомогательные процессы – вспомогательные;
– организационные процессы – управленческие, организационные.

Тринадцатипроцессная модель (рис. 8), часто используемая отечественными консультантами, как при проведении семинаров, так и в реальных проектах, составлена по данным Международной бенчмаркинговой палаты (International Benchmarking Clearinghouse) [19]. Блок «Производство и поставка продуктов и услуг» обычно разбивается на составляющие: «производство продукции» и «оказание услуг».

Рис. 8. Тринадцатипроцессная модель

Восьмипроцессная модель (рис. 9, табл. 3) была разработана и успешно применяется сотрудниками консалтинговой компании BKG Profit Technology [19].

Рис. 9. Восьмипроцессная модель

Таблица 2

Восьмипроцессная модель

Название бизнес-процесса	Описание бизнес-процесса	Результат бизнес-процесса
Выработка согласованных условий деятельности	Все виды деятельности по определению «правил игры» бизнес-системы, т. е. стратегическое планирование, политика, регламенты деятельности, в том числе организационная структура компании	Регламенты системы управления
Развитие	Все виды деятельности по разработке нового продукта, выработке производственных технологий, в том числе требований системы качества. При определенных обстоятельствах, например для небольших бизнес-систем, этот процесс может сливаться с процессом выработки согласованных условий деятельности	Производственные регламенты
Продажи	Все виды деятельности, связанные с формированием потока обязательств между бизнес-системой и внешней средой, нацеленные на предоставление внешней среде ценностей, востребуемых ею	Поток обязательств, в общем виде – дебиторская задолженность и планы предприятия
Производство	Все виды деятельности, связанные с переработкой ресурсов в готовую продукцию в таких объемах и такого качества, которые соответствуют требованиям внешней среды	Готовая продукция
Воспроизводство ресурсов	Все виды деятельности, направленные на получение из внешней среды производственных ресурсов в количестве и качеством, соответствующим требованиям процесса «производство»	Ресурсы (комплектующие, материалы, информация и т. д.) в производстве
Воспроизводство механизмов	Все виды деятельности, направленные на обеспечение бизнес-системы основными средствами и	Работоспособные основные средства в

Окончание табл. 2

Название бизнес-процесса	Описание бизнес-процесса	Результат бизнес-процесса
	оборудованием, в количествах и по качеству соответствующих требованиям производства востребуемой внешней средой ценности	эксплуатации
Расчеты	Все виды деятельности, связанные с обменом готовой продукции на денежные средства, с работой дебиторской и кредиторской задолженностями, распределением денежных средств	Чистый денежный поток
Воспроизводство компетенции	Все виды деятельности, связанные с обеспечением бизнес-системы необходимыми компетенциями (знаниями, опытом, умениями) и их носителями (персоналом)	Персонал, обладающий необходимым уровнем компетенции

Третий подход основывается на описанной М. Портером цепочке создания ценности (рис. 10) [19]. В цепочке выделяются основные бизнес-процессы, обеспечивающие операционный цикл производства, выполняющиеся последовательно и поддерживающие бизнес-процессы, обеспечивающие функционирование бизнес-системы и сопровождающие создание продукта на всем протяжении его жизненного цикла.

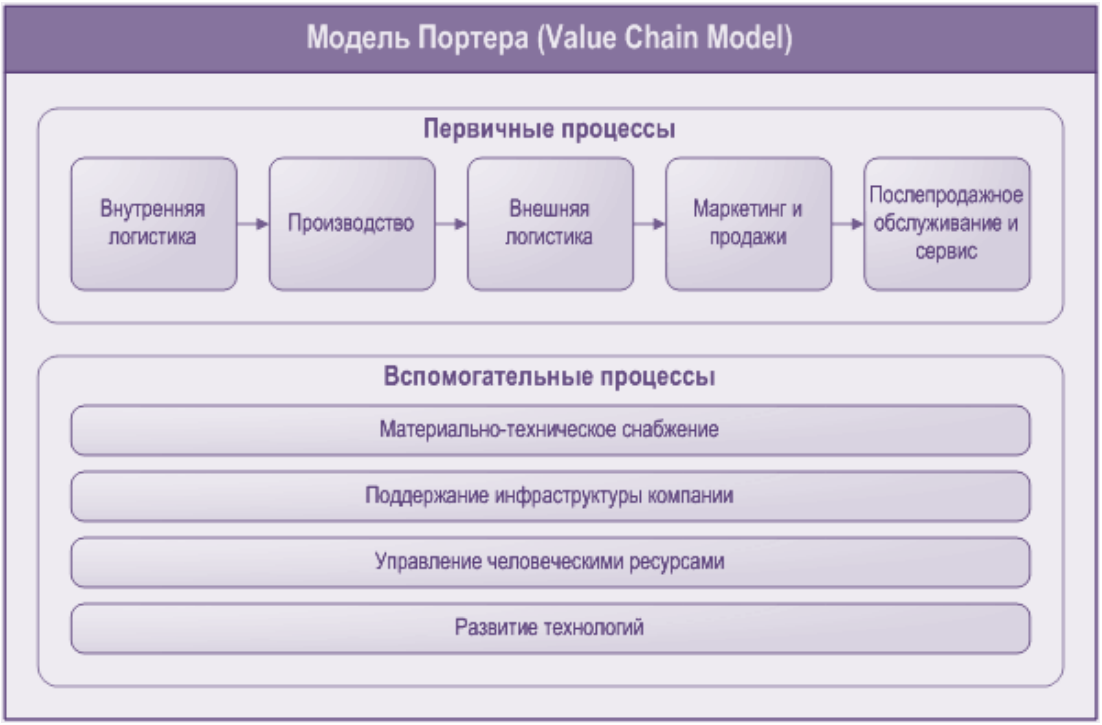

Рис. 10. Модель Портера

М. Портер указал, что покупатели приобретают не продукт как таковой, а его ценность лично для себя, и поэтому, чтобы предприятие могло точно определить свои конкурентные преимущества, необходимо рассмотреть всю последовательность процесса создания именно этой ценности. Иными словами, цепочка создания ценности представляет собой инфраструктуру, показывающую значимость бизнес-процессов [19]. Первичными являются бизнес-процессы,

предназначенные непосредственно для создания результатов деятельности предприятия – ценности для клиента. Вторичные бизнес-процессы играют вспомогательную роль, обеспечивая необходимую инфраструктуру и средства управления при выполнении первичных бизнес-процессов. При решении вопроса о границах процессов М. Портер предположил, что границы звеньев цепочки, а, следовательно, и бизнес-процессов, находятся там, где каждый внутренний подпроцесс что-то добавляет к ценности продукта. Из этого предположения М. Портера, кстати сказать, вытекает интересный вывод: не существует стандартного списка бизнес-процессов, каждое предприятие должно разработать собственный перечень основных бизнес-процессов, так как продукт, как ценность для клиента, для каждого предприятия уникален.

Методологии описания бизнес-процессов

Моделирование бизнес-процессов – это отражение субъективного видения реально существующих в организации процессов при помощи графических, табличных, текстовых способов представления.

Методология моделирования бизнес-процессов (Business Process Modeling) – совокупность методов и принципов построения моделей бизнес-процессов.

Модель «как есть» (от «as is» – англ.) – это модель бизнес-процесса, построенная на основе субъективного видения бизнес-процесса, существующего в организации.

При построении модели «как есть» важно учитывать два фактора – субъективности и актуальность модели. В крупных организациях постоянно происходят изменения. Модель процессов может стать неактуальной (несоответствующей) уже через несколько месяцев после ее создания. Поэтому описание процесса должно использоваться в рабочих документах по процессу, постоянно подвергаться корректировке с целью обеспечения соответствия реальной деятельности.

Под методологией (нотацией) создания модели (описания) бизнес-процесса понимается совокупность способов, при помощи которых объекты реального мира (например, деятельность организации) и связи между ними представляются в виде модели.

В практике используют большое количество методологий описания бизнес-процессов, разрабатываемых IT-компаниями. Большинство из них базируются на сочетании следующих основных моделей: блок-схемы; нотация IDEF0; методология IDEF3; нотация ARIS eEPS; нотация DFD; стандарт UML.

Методы моделирования бизнес-процессов [10]:

– Flow Chart Diagram (диаграмма потока работ) – способ графического описания работы с применением особых символов для каждой операции, набора данных, единицы оборудования, исполнителя. В результате на схеме демонстрируется логическая последовательность всех операций. Это гибкий подход, он дает возможность при необходимости рассмотреть один комплекс действий сразу в нескольких вариантах.

– Data Flow Diagram – изображение передачи данных между операциями, для характеристики информационной стороны бизнес-процесса. Это позволяет

наблюдать данные на входе в систему и в каждую операцию в отдельности, и соответствующую информацию на выходе. Также в ней отображается, какими способами сведения претерпевают изменения и где хранятся. Деятельность компании раскладывается на логические информационные уровни, причем базовая схема улучшается добавлением подробных описаний подпроцессов, тоже имеющих свою внутреннюю структуру.

– Role Activity Diagram (диаграмма ролей). Под ролью здесь понимается каждый элемент, выполняющий ту или иную функцию. Каждая часть описывается, и анализируется отдельно, а затем рассматривается их взаимодействие.

– IDEF (Integrated Definition for Function Modeling) – это целый набор аналитических средств, применяемых не только в управлении бизнесом, но и во многих других сферах. Чаще всего встречаются варианты IDEF0 и IDEF3. Первый из этих вариантов представляет собой модель функций, причем сложные функции делятся на более простые составляющие, а затем различные блоки логически объединяются посредством стрелок. При использовании IDEF3 речь идет о «поведенческом» описании: демонстрируется поток работ либо переходные состояния объектов.

– Цветные сети Петри – график, на котором представлены действия и события, символизирующие переход из одной стадии в другую. Таким образом, можно увидеть, что приводит к тем или иным изменениям, насколько быстро и эффективно.

– Unified Modeling Language – графический язык для визуализации, специфицирования, конструирования и документирования процессов и систем. Комплекс из девяти видов диаграмм, описывающих разные аспекты: классы, объекты, прецеденты, последовательности, кооперации, состояния, деятельность, компоненты, развертывание. В результате получается представление очередности действий сотрудников и работы различных объектов внутри организации. Схема может разветвляться, в ней отмечаются разнообразные условия и исключения из правил.

– ARIS (Architecture of Integrated information Systems) – методология и соответствующее семейство программных продуктов. Они используются для структурированного описания, анализа и последующего совершенствования бизнес-процессов предприятия. Система наглядно показывает правила деятельности предприятия и значения показателей результативности. Так можно определить желаемые характеристики работы компании, совершенствовать архитектуру, улучшить процессы, рационально распределять ресурсы. Инструмент определяет весь цикл разработки – анализ требований, спецификация информационной системы и описание физической реализации.

Подробнее с процессами построения моделей бизнес процессов можно ознакомиться в работах:

– Бизнес-моделирование: IDEF0, DFD, IDEF3, FISHBONE, FTA : учебное пособие [2];

– Гаврилова И.В. Свободное программное обеспечение для управления бизнес-процессами [4]

– Гаврилова И.В. Система управления бизнес-процессами Activity BPM [5];

– Назарова О.Б. Моделирование бизнес-процессов [13];

– Новикова Т.Б. Aris: теория и практика бизнес-моделирования [14];

– Совершенствование методов построения причинно-следственных диаграмм для решения задач управления в организационных системах [21];

– Чусавитина, Г.Н., Давлеткиреева, Л.З. Анализ и установление уровня зрелости информационной инфраструктуры организации для управления непрерывностью бизнеса [24].

Задание 2

Проранжировать бизнес-процессы и активы по степени критичности для бизнеса.

Критические процессы – процессы, ненадлежащая организация которых или несоблюдение требований к их выполнению могут представлять фактическую или потенциальную опасность для обеспечения качества продукции и, следовательно, для эффективности бизнеса.

Критические процессы должны незамедлительно корректироваться или улучшаться. В разряд критических может попасть любой процесс.

Выявление критических процессов осуществляется в ходе текущей деятельности или по результатам аудиторских проверок. При этом следует отметить, что если ключевые процессы отражают внешние по отношению к организации воздействия, то критические процессы являются отражением сугубо внутренних воздействий.

В строгом смысле данных определений критерий критической важности того или иного процесса – невозможность восстановления бизнеса в случае прерывания данного процесса на некий срок максимально допустимого времени прерывания (МДВП). Для любого процесса можно экспертно оценить его «персональный» МДВП. Для некоторых оно будет бесконечным – это процессы заведомо не критичные. Далее можно ранжировать критичные процессы по их «персональным» МДВП – часть опердня, опердень, два опердня и т.д.

Ранжирование бизнес-процессов по степени критичности может быть осуществено следующими способами:

– экспертная оценка (опрос сотрудников и руководства, выбор среднего значения)

– разработка критериев важности и экспертная оценка каждого критерия

– простое сопоставление бизнес-процессов и «критических факторов успеха» (т.е. вклад каждого бизнес-процесса в достижение стратегических целей компании, реализацию миссии)

– весовое сопоставление бизнес-процессов и «критических факторов успеха»

Пример выполнения практической работы 2

Задание 1. Описать основные бизнес-процессы и активы организации.

Служба охраны

1. Допуск сотрудников в здание
2. Допуск клиентов в здание
3. Просмотр камер видеонаблюдения

Технический отдел

1. Организация работы внутренней и внешней сети
2. Организация работы компьютерной инфраструктуры
3. Приобретение и сопровождение технических средств
4. Обучение специалистов по вопросам применения технических средств
5. Монтаж и модернизация компьютерных и телефонных сетей
6. Профилактика, техническое обслуживание, модернизация и мелкий ремонт СВТ.
7. Формирование заявок на оборудование
8. Учет приобретаемых и выданных расходных материалов

Отдел работы с клиентами

1. Реализация АИС
2. Удержание имеющихся клиентов
3. Поиск новых клиентов
4. Маркетинг

Отдел проектов

1. Разработка АС
2. Формирование требований
3. Разработка ТЗ
4. Разработка концепции АС

Отдел АСУТП

1. Разработка ПС в соответствии с ТЗ
2. Выполнение работ в соответствии с гарантийными обязательствами
3. Послегарантийное обслуживание
4. Обновление АИС
5. Подготовка объекта к автоматизации
6. Проведение предварительных испытаний
7. Проведение опытной эксплуатации
8. Пуско-наладочные работы

Отдел бухгалтерии

1. Начисление заработной платы
2. Начисление и выплата налогов

3. Подготовка к аудиторской проверке
4. Ведение бухгалтерской отчетности

Руководство компании ЗАО «МагПромАвтоматика»
1. Контроль деятельности отделов
2. Составление стратегии развития организации
3. Контроль за реализацией стратегии

Задание 2. Проранжировать бизнес-процессы и активы по степени критичности для бизнеса.

После описания организации необходимо проранжировать бизнес-процессы и таким образом выявить самые критичные для подразделения процессы. В ходе ранжирования бизнес процессы распределились следующим образом:

– Реализация АИС;
– Разработка ПС в соответствии с ТЗ;
– Выполнение работ в соответствии с гарантийными обязательствами;
– Удержание имеющихся клиентов;
– Организация работы компьютерной инфраструктуры Поиск новых клиентов;
– Ведение бухгалтерской отчетности;
– Начисление заработной платы.

Практическая работа 3.
Оценка воздействия на бизнес по методу BIA

Оценка влияния прерываний на бизнес (Business Impact Analysis, BIA) является ключевой темой непрерывности бизнеса и состоит в функциональном анализе того, как прерывания повлияют на деятельность организации.

К задачам BIA относят:

– определение ценности каждого бизнес-процесса;

– идентификацию и ранжирование прерываний каждого бизнес-процесса;

– приоритизацию бизнес-процессов;

– оценку ресурсов на обеспечение непрерывности бизнес-процессов

BIA (business impact analysis – анализ влияния на бизнес) – это функциональный анализ, в процессе которого команда собирает данные, проводя интервью и анализируя документальные источники; документирует бизнес-функции, действия и транзакции; разрабатывает иерархию бизнес-функций; и, наконец, определяет уровень критичности каждой отдельной функции с помощью порядка классификации.

Максимально допустимое время простоя:

– Нарушение работы и снижение производительности

– Возмещение финансовых убытков (financial consideration)

– Ответственность, установленная законодательством и регуляторами

– Репутация

Нельзя полностью понимать все бизнес-процессы компании, какие действия и ресурсы нужны для работы этих процессов. Определим, кто их сотрудников будет участвовать в процессе сбора данных для BIA. Должны быть оформлены схемы процессов, которые будут использоваться на этапе проведения BIA и на других этапах разработки плана. После завершения этапа сбора данных, необходимо провести их анализ для определения, какие процессы, устройства и операционные функции являются критичными для компании. Например, если система является автономной, не влияет на другие системы и имеет невысокую критичность, она может быть классифицирована, как восстанавливаемая на второй или третьей фазе процесса восстановления. Соответственно, эта система не будет восстанавливаться до тех пор, пока не завершится восстановление и запуск в работу более критичных систем и ресурсов. Угрозы могут быть рукотворными, природными или техническими. Рукотворными угрозами могут быть поджоги, террористические акты или просто ошибки, приводящие к серьезным последствиям. Природными угрозами могут быть торнадо, наводнения, ураганы или землетрясения. Техническими угрозами могут быть повреждения данных, перебои электроснабжения, неисправности устройств, нарушения работы коммуникационных каналов. Важно выявить все возможные угрозы и рассчитать вероятность их реализации. Некоторые угрозы могут показаться неразумными и надуманными, например, злоумышленные действия сотрудников, вандализм, протесты сотрудников, атаки хакеров и т.п.,

но эти угрозы также должны быть идентифицированы. Для анализа угроз лучше использовать подход, основанный на сценариях их реализации. Это позволит наиболее полно учесть при подготовке плана влияние этих угроз на задачи бизнеса, подразделения и критичные операции компании. Чем больше угроз учтет компания при планировании, тем лучше она будет готова к наступлению чрезвычайных ситуаций.

Шаги BIA.

1. Подбор людей для опроса в процессе сбора данных.
2. Выбор метода сбора данных (анкетирование, исследование, количественный и качественный подходы).
3. Идентификация критичных для компании бизнес-функций.
4. Идентификация ресурсов, которые необходимы для выполнения этих функций.
5. Расчет времени, в течение которого эти бизнес-функции могут «прожить» без этих ресурсов.
6. Выявление уязвимостей и угроз для этих бизнес-функций.
7. Расчет рисков для каждой отдельной бизнес-функции.
8. Подготовка документа по результатам BIA и предоставление его руководству.

Далее необходимо проанализировать сценарии, которые приведут к следующим последствиям:

– Неисправность или недоступность оборудования
– Недоступность водоснабжения, коммунальных услуг, отопления, вентиляции, электроэнергии (utilities)
– Недоступность (невозможность использования) здания
– Недоступность (неработоспособность) критичного персонала
– Недоступность (неработоспособность) производителей или поставщиков услуг
– Повреждение программного обеспечения и/или данных

Следующим шагом анализа рисков является определение ценности активов, на которые может оказать влияние каждая из угроз. Это поможет сделать план экономически целесообразным. Определение ценности активов не так однозначно, как может показаться. Ценность актива – это не просто сумма денег, которую за него заплатили. Должна быть учтена роль (значение) этого актива для компании, а также трудозатраты на его воссоздание (например, если это часть программного обеспечения). Кроме того, в определении ценности актива должны учитываться вопросы ответственности компании в случае повреждения актива или нарушения его безопасности. Должна быть собрана количественная и качественная информация в отношении воздействия на бизнес фактов реализации различных угроз, собранная информация должна быть надлежащим образом проанализирована и интерпретирована с целью максимально точного понимания последствий воздействия этих угроз. При этом воздействие может быть экономическим, функциональным (операционным) или одновременно и

тем, и другим. Результаты анализа следует передать наиболее квалифицированным людям в компании для рассмотрения, чтобы они подтвердили, что получены адекватные результаты, описывающие реальные риски, перед лицом которых стоит компания, и их воздействия на бизнес. Это поможет сразу исключить все несущественные данные и обеспечить максимально полное понимание всех возможных воздействий на бизнес.

К выявленным угрозам по отдельности должны быть применены критерии потерь (loss criteria). Среди этих критериев могут быть следующие:

- Ущерб репутации и общественному доверию
- Потеря конкурентных преимуществ
- Повышение операционных расходов
- Нарушение контрактных обязательств
- Нарушение законодательства и требований регуляторов
- Отложенные расходы
- Потеря доходов
- Снижение производительности

Эти прямые и косвенные потери должны быть надлежащим образом учтены.

Например, если команда BCP рассматривает угрозу террористического акта, важно определить, на какие бизнес-функции это скорее всего будет направлено, на какие бизнес-функции будет оказано воздействие, насколько применим для этого случая (прямо или косвенно) каждый из пунктов перечня критериев потерь. Для отдельных бизнес-процессов и компании в целом может быть критично время восстановления. Например, это может быть применимо к деятельности по поддержке клиентов, которая может быть остановлена не более, чем на два дня. Если поддержка клиентов будет остановлена на пять дней, компания может прекратить свое существование.

После идентификации критичных функций, необходимо точно определить, что требуется для работы отдельным бизнес-процессам, реализующим эти критичные функции. Среди необходимых им ресурсов не обязательно будут только компьютерные системы, они могут требовать наличия определенного персонала, выполнения определенных процедур и задач, наличия запасов сырья, поддержки производителей. Команда должна понять, какое влияние на эти процессы окажет недоступность одного или более из необходимых им ресурсов, отсутствие каких ресурсов полностью остановит выполнение соответствующей критичной функции.

В процессе BIA, команда идентифицирует критичные для компании системы, необходимые для ее функционирования, и рассчитывает допустимое для компании время их простоя, вызванного различными неблагоприятными событиями. Это время называется максимально допустимым временем простоя (MTD – maximum tolerable downtime).

Ниже представлены некоторые значения MTD, которые могут быть использованы компанией:

- Второстепенная система. MTD = 30 дней

– Обычная система. MTD = 7 дней
– Важная система. MTD = 72 часа
– Необходимая система. MTD = 24 часа
– Критичная система. MTD = менее 1 часа

Каждая бизнес-функция и каждый актив должны быть помещены в одну из этих категорий, в зависимости от времени, в течение которого компания может жить без этой функции или актива. Это поможет компании обоснованно выбрать необходимое ей решение для организации резервного копирования, обеспечивающее гарантии доступности этих ресурсов. Например, если неработоспособность выделенной линии в течение 3 часов обойдется компании в $130 000, эту выделенную линию следует считать критичной, и компании следует организовать резервный канал связи от другого провайдера. Если недоступность сервера в течение 10 дней нанесет компании ущерб всего на $250, его следует считать второстепенным, и компании не нужен полностью готовый к работе резервный сервер, который можно будет сразу же включить в работу при неисправности основного сервера. Вместо этого, компания может решить заключить соглашение со специализированной компанией (аутсорсинг), который, в соответствии с согласованным SLA (service level agreement – соглашение об уровне услуг), восстановит работу этого сервера за 8 дней.

Команда BCP должна попытаться продумать максимально возможное количество событий, которые могут произойти и нанести ущерб компании. При этом команда BCP должна понимать, что обеспечить защиту от всех возможных событий и сценариев – нереально. Хорошая подготовка к наводнению, землетрясению, террористической атаке или удару молнии не так важна, как хорошая подготовка к нарушению или полной остановке критичных бизнес-функции. Компания должна быть готова к повреждению любого (или всех) из своих бизнес-ресурсов, а не сосредотачиваться на отдельных событиях, которые могут нанести ей ущерб.

Взаимозависимости

Важно рассматривать компанию в виде сложного организма. В компании используется множество различных типов оборудования, работают люди, выполняются различные задачи, созданы различные подразделения, организованы коммуникационные каналы и интерфейсы связи с внешним миром. Самой большой сложностью при правильном планировании непрерывности является понимание всех этих компонентов и их взаимоотношений. Команда может разработать планы резервного копирования и восстановления данных, установить резервное оборудование, обучить сотрудников вручную выполнять автоматизированные задачи и предусмотреть дополнительные источники питания. Но если нет четкого понимания, как все эти компоненты будут совместно работать в другой среде, позволяя получить на выходе тот же продукт, это может оказаться пустой тратой времени и денег.

Следующие взаимосвязи и взаимозависимости задач должны быть выявлены командой BCP и учтены в разрабатываемом плане непрерывности:

– Определение важнейших бизнес-функций и поддерживающих их подразделений.

– Определение взаимозависимостей между этими функциями и подразделениями.

– Выявление всех возможных нарушений (аварий, разрушений) которые могут оказать воздействие на механизмы, необходимые этим подразделениям для функционирования.

– Выявление и документирование потенциальных угроз, которые могут нарушить взаимодействие подразделений между собой.

– Сбор количественной и качественной информации, относящейся к этим угрозам.

– Обеспечение альтернативных методов восстановления функциональности и коммуникаций.

– Подготовка краткого и понятного описания для каждой угрозы и соответствующей информации.

Задание

Оценить воздействие на бизнес по методу BIA

Пример выполнения практической работы 3

Задание. Оценить воздействие на бизнес по методу BIA

Оценка существующих угроз для критичного бизнес-процесса «Реализация АИС»

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 была построена модель модели управлении процессом обеспечения непрерывности бизнеса и модель критичного бизнес-процесса «Реализация АИС» (рис. 1, 2)

Определены следующие угрозы критичного бизнес-процесса «Реализация АИС»:

- отключение электричества;
- потеря персонала;
- компьютерные атаки;
- отказы и сбои аппаратных средств;
- террористические акты;
- пожары;
- наводнения;
- землетрясения.

Оценка ресурсов, необходимых для ВСМ

- Персонал (численность, квалификация): требуется человек с высокой квалификацией, со знанием процедур обеспечения информационной безопасности и непрерывности бизнеса
- Необходимые площади и помещения: 2-3 помещения общей площадью 50 кв.м.
- Денежные ресурсы: 500 000 руб.
- Основные производственные средства и технологии: датчики, КИПиА, исполнительные устройства, контроллеры, серверное оборудование, промышленные и персональные компьютеры, ноутбуки, активное и пассивное сетевое оборудование, шкафное оборудование (серверные, сетевые, полевые), инженерная инфраструктура, офисное оборудование, комплектующее оборудование и материалы, программное обеспечение различного назначения.
- Информационные активы: персональные данные; стратегическая информация, необходимая для достижения бизнес-целей; коммерческая тайна; служебная тайна и т.д.)

Рис. 1. Разработка модели управлении процессом обеспечения непрерывности бизнеса

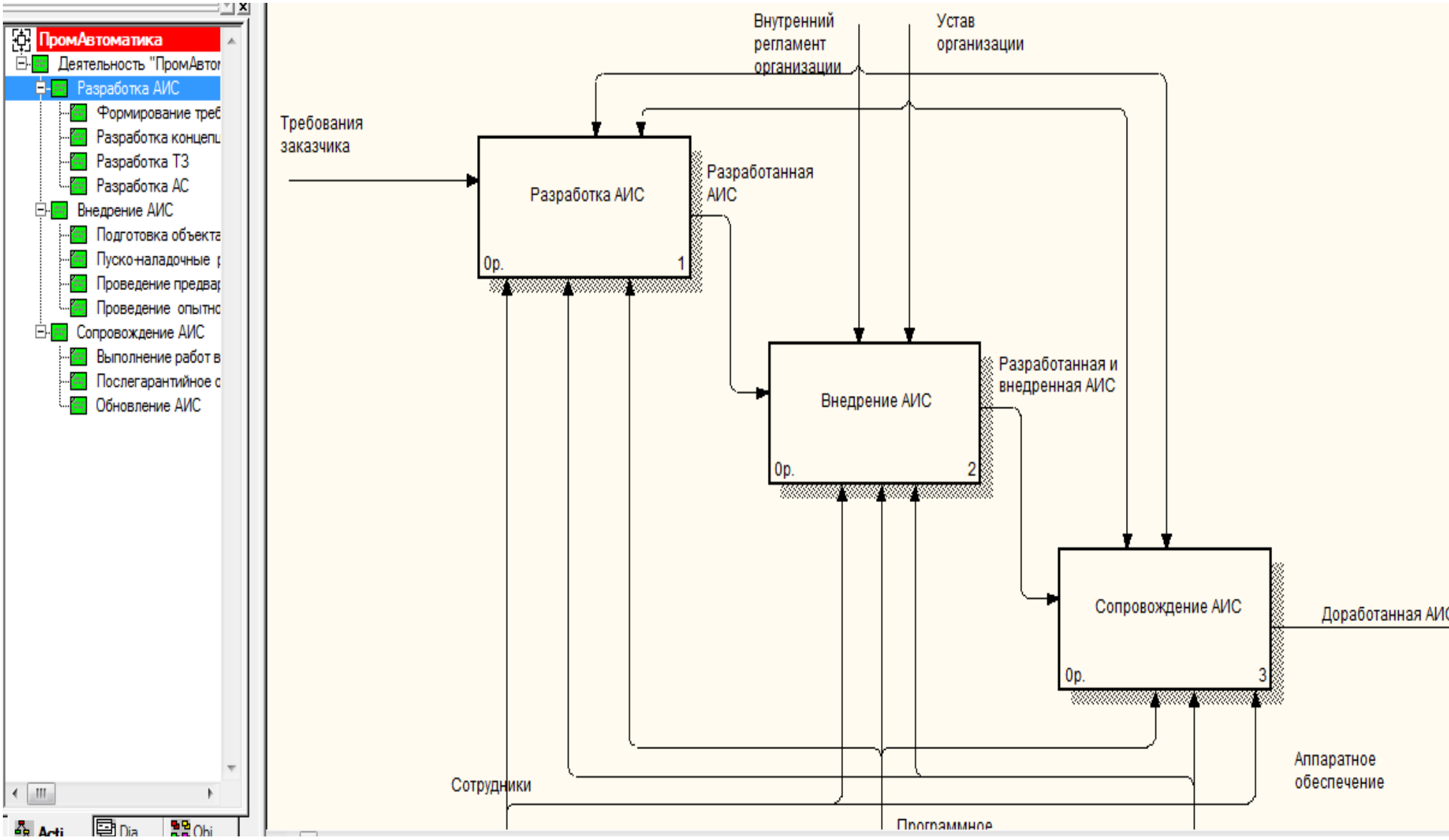

Рис. 2. Моделирование критичного бизнес-процесса «Реализация АИС»

Оценка рисков, RA

Описание риска (угрозы)	Уязвимости	Возможный источник угрозы	Вероятные последствия – результаты реализации угрозы (сценарии)
Перегрузка приложения реализации АИС	Отсутствие механизма защиты от перегрузки канала связи. Архитектура приложения, неоптимизированная для высоких нагрузок	Рабочий персонал	Невозможность проведения реализации АИС; изменение базы реализации АИС. Вред репутации организации
Пожар	Неисправность системы пожаротушения	Рабочий персонал	Пожар, все сгорит
Потеря персонала	Неукомплектованность кадрами	Руководство	Вред организации, снижение производства
Компьютерные атаки	Действие вредоносного ПО	Рабочий персонал	Потеря АИС
Террористические акты (взрывы)	Отсутствие антитеррористического плана	Любой человек	Вред организации и всему персоналу

Практическая работа 4.
Ранжирование критически важных бизнес-процессов

При определении ценности бизнес-процессов для информационных систем могут быть зафиксированы значения ряда технических показателей:

– MTPD (Maximum Tolerable Period of Disruption, максимально приемлемый период прерывания бизнеса) – период времени, по истечении которого неблагоприятные последствия, возникшие в результате прерывания бизнеса, становятся неприемлемыми;

– RTO (Recovery Time Objective, целевое время восстановления) – период времени после произошедшего прерывания, в течение которого должен быть восстановлен минимальный уровень деятельности организации, а также поддерживающие его системы, прикладные программы и функции;

– RPO (Recovery Point Objective, целевая точка восстановления) – период времени, за которое должны быть восстановлены данные после прошедшего прерывания.

– LBC (англ. Level of business continuity) – «уровень непрерывности бизнеса», описывающий какую долю штатной нагрузки должен обеспечивать бизнес-процесс в случае чрезвычайной ситуации

Полагается, что: RTO < MTPD.

В литературе можно встретить другие показатели, например:

– MAO (Maximum Acceptable Outage), MAD (Maximum Allowable Downtime), MTD (Maximum Tolerable Downtime) – допустимое время простоя, применяемое в области непрерывности бизнеса в качестве синонима MTPD.

– MDL (Maximum Data Loss) – в качестве синонима RPO.

Можно показать, что указанные показатели будут влиять на выбор решений по восстановлению бизнес-процессов или данных. Например, если RTO = 8 час, то, скорее всего, ИТ-специалисты успеют полностью переустановить, например, системное ПО и восстановить данные из резервных копий, если RTO составляет 5 минут, то здесь речь уже будет идти о параллельно работающих элементах системы с дублированием данных.

Задание

Провести ранжирование критически важных бизнес-процессов

Пример выполнения практической работы 4

Задание. Провести ранжирование критически важных бизнес-процессов

Рассчитаем допустимое время восстановления бизнес-процессов

Бизнес-процесс	Время восстановления
Реализация АИС	TPD max =2 часа; RTO max = 4 часа; LBC = 75%
Разработка ПС в соответствии с ТЗ	TPD max =2 часа; RTO max = 30 минут; LBC = 50%
Выполнение работ в соответствии с гарантийными обязательствами	TPD max =5 дней; RTO max = 2 часа; LBC = 75%
Удержание имеющихся клиентов	TPD max = 30 минут; RTO = 1 час; LBC = 20%
Организация работы компьютерной инфраструктуры	TPD max = 15 минут; RTO = 3 часа; LBC = 50%
Поиск новых клиентов	TPD max = 2 часа; RTO = 3 часа; LBC = 70%
Ведение бухгалтерской отчетности	TPD max=4 часа; RTO max = 1 час; LBC = 50%
Начисление заработной платы	TPD max = 2 дня; RTO = 6 часов; LBC = 70%

Таким образом, наибольшую длительность на восстановление имеет процесс «Начисление заработной платы». Высокий уровень непрерывности бизнеса имеет процесс «Реализация АИС».

Практическая работа 5
Оценка угроз критическим видам деятельности организации

В зависимости от целей применения менеджмента непрерывности бизнеса необходимо проводить анализ риска с точки зрения непрерывности критических видов деятельности организации и риска их нарушения. Критические виды деятельности должны поддерживаться такими ресурсами, как персонал, производственные площади, технологии, информация, запасы и причастные стороны. Организация должна оценить потенциальные угрозы для этих ресурсов, уязвимость каждого вида ресурса и потенциальное воздействие при превращении угрозы в инцидент, который может вызвать нарушение ее деятельности.

Выбор подхода к оценке риска – это самостоятельное решение организации, однако важно, чтобы этот подход соответствовал всем требованиям организации.

ИСО/МЭК 27001:2005 Information technology - Security techniques - Information security management systems - Requirements (ИСО/МЭК 27001:2005 Информационная технология. Методы безопасности. Информационные системы управления безопасности. Требования) устанавливает структуру подхода к оценке риска и обязательные элементы, которые должны включать процесс оценки риска. Типовыми элементами являются:

– определение критериев принятия риска. Должны быть описаны условия, при которых организация может принять риск;

– идентификация приемлемых уровней риска. Независимо от выбранного подхода к оценке риска организация должна идентифицировать приемлемый риск;

– анализ риска.

Конкретные угрозы могут быть описаны как опасные события или действия, которые могут в какой-то момент оказать негативное воздействие на ресурсы, например, такие угрозы, как пожар, наводнение, нарушение энергоснабжения, потеря персонала, невыход персонала на работу, компьютерные вирусы или отказ компьютерных аппаратных средств.

Уязвимые места – это недостатки («слабые места») в ресурсах, которые могут подпасть под воздействие угроз, например, неустойчивость работы одного элемента системы, отдельные несоответствия в противопожарной защите, неустойчивость к скачкам напряжения электросети, неукомплектованность персоналом, незащищенность или неустойчивость отдельных частей информационных технологий и т.д.

Воздействие на бизнес может явиться следствием воздействия опасных событий на уязвимые места.

Классификация источников угроз

Источник угрозы	Описание
Класс 1. Источники угроз, связанные с неблагоприятными событиями природного, техногенного и социального характера	
Пожар	Неконтролируемый процесс горения, сопровождающийся уничтожением материальных ценностей и создающий опасность для жизни людей. Возможные причины: поджог, самовозгорание, природное явление
Природные катастрофы, чрезвычайные ситуации и стихийные бедствия	Природные явления разрушительного характера (наводнения, землетрясения, извержения вулканов, ураганы, смерчи, тайфуны, цунами и т.д.)
Техногенные катастрофы	Разрушительный процесс, развивающийся в результате нарушения нормального взаимодействия технологических объектов между собой или с компонентами окружающей природной среды, приводящий к гибели людей, разрушению и повреждению объектов экономики и компонентов окружающей природной среды
Нарушение внутриклиматических условий	Негативное изменение климатических условий в помещениях, где расположены технические средства и/или находится персонал: значительные изменения температуры и влажности, повышение содержания углекислого газа, пыли и т.п. Возможные последствия: сбои, отказы и аварии технических средств, снижение работоспособности и нанесение ущерба здоровью персонала, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Нарушение электропитания	Нарушение или снижение качества электропитания. Возможные причины: техногенная катастрофа, стихийное бедствие, природное явление, террористический акт, пожар и т.п. Возможные последствия: сбои и отказы технических средств
Нарушение функционирования систем жизнеобеспечения	Сбои и аварии в системах водоснабжения, канализации, отопления
Угроза здоровью персонала	Угроза здоровью персонала в результате радиационных, биологических, механических, термических, химических и иных воздействий со стороны окружающей среды, объектов инженерной инфраструктуры, технических средств, пищевые отравления, производственный травматизм. Возможные причины: техногенные или природные катастрофы, аварии объектов инженерной инфраструктуры, неисправность оборудования, несоблюдение правил техники безопасности и охраны труда, санитарных правил и т.д. Возможные последствия: нехватка персонала, денежные выплаты, судебные разбирательства
Класс 2. Источники угроз, связанные с деятельностью террористов и лиц, совершающих преступления и правонарушения	
Нарушения общественного порядка, вандализм, массовые беспорядки, политическая нестабильность	Уничтожение или повреждение имущества организации

Источник угрозы	Описание
Террористические действия	Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения организацией, а также угроза совершения указанных действий в тех же целях
Промышленный шпионаж	Передача, собирание, похищение или хранение информационных активов организации для использования их в ущерб организации
Запугивание и шантаж	Принуждение персонала организации к осуществлению несанкционированных действий, заключающееся в угрозе разоблачения, физической расправы или расправы с близкими
Социальный инжиниринг	Умышленные действия сторонних лиц, преследующих мошеннические цели, реализуемые посредством обмана, введения в заблуждение работников организации. Возможные последствия: ошибки работников, нарушение свойств, утрата информационных активов, нарушение непрерывности процессов, снижение качества информационных услуг (сервисов)
Класс 3. Источники угроз, связанные с деятельностью поставщиков/провайдеров/партнеров	
Зависимость от партнеров/клиентов	Зависимость от партнеров заставляет организацию полагаться на их информационную безопасность, организация должна быть уверена, что партнер сможет обеспечить должный уровень безопасности либо учитывать данный источник угроз
Ошибки, допущенные при заключении контрактов с провайдерами внешних услуг	Неточности и неопределенности в договоре с провайдером внешних услуг, которые могут создавать проблемы в работе заказчика
Нарушения договорных обязательств сторонними (третьими) лицами	Невыполнение со стороны третьих лиц взятых на себя обязательств по качеству, составу, содержанию и/или порядку оказания услуг, поставки продукции и т.д. Например, невыполнение требований разработчиками, поставщиками программно-технических средств и услуг или внешними пользователями
Ошибки в обеспечении безопасности информационных систем на стадиях жизненного цикла	Ошибки в обеспечении безопасности при разработке, эксплуатации, сопровождении и выводе из эксплуатации информационных систем
Разработка и использование некачественной документации	Некачественное выполнение документированного описания технологических процессов обработки, хранения, передачи данных, руководств для персонала, участвующего в этих технологических процессах, а также описания средств обеспечения ИБ и руководств по их использованию
Использование программных средств и информации без гарантии источника	Использование в информационной системе организации непроверенных данных или нелицензионного программного обеспечения
Класс 4. Источники угроз, связанные со сбоями, отказами, разрушениями/повреждениями программных и технических средств	
Превышение допустимой	Неумышленное превышение допустимой нагрузки на вы-

Источник угрозы	Описание
нагрузки	числительные, сетевые ресурсы системы. Выполнение работниками объема операций большего, чем это допускается психофизиологическими нормами. Возможные причины: малая вычислительная и/или пропускная мощность, неправильная организация бизнес-процессов. Возможные последствия: сбои и отказы технических средств, нарушение доступности технических средств, ошибки персонала, нанесение вреда здоровью
Разрушение/повреждение, аварии технических средств и каналов связи	Физическое разрушение/повреждение технических средств (канала связи) или определенное сочетание отказов его элементов, приводящее к нарушениям функционирования, сопряженным с особо значительными техническими потерями, делающее невозможным функционирование технического средства (канала связи) в целом в течение значительного периода времени. Возможные причины: действие внешних (физический несанкционированный доступ, террористический акт, техногенная катастрофа, стихийное бедствие, природное явление, массовые беспорядки) и/или внутренних (значительные отказы элементов технических средств) факторов. Возможные последствия: нарушение свойств информационных активов, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Сбои и отказы программных средств	Нарушение работоспособности программных средств. Возможные причины: недопустимое изменение параметров или свойств программных средств под влиянием внутренних процессов (ошибок) и/или внешних воздействий со стороны вредоносных программ, оператора и технических средств. Возможные последствия: нарушение свойств информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Сбои и отказы технических средств и каналов связи	Прерывание работоспособности технических средств или невозможность выполнения ими своих функций в заранее установленных границах. Возможные причины: недопустимое изменение характеристик технических средств под влиянием внутренних процессов, сложность технических средств, нехватка персонала, недостаточное техническое обслуживание. Возможные последствия: сбои, отказы программных средств, аварии систем, нарушение доступности информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Нарушения функциональности криптографической системы	Случайное или намеренное неправильное управление криптографическими ключами, криптографическими протоколами и алгоритмами, программно-аппаратными средствами систем криптографической защиты информации, приводящее к потере конфиденциальности, целостности и доступности информации, нарушению неотказуемости приема-передачи информации, блокировке функционирования платежных и информационных систем организации

Источник угрозы	Описание
Нарушения функциональности архивной системы	Нарушение конфиденциальности и целостности архивных данных и/или непредоставление услуг архивной системой (нарушение доступности) вследствие случайных ошибок пользователей или неправильного управления архивной системой, а также вследствие физических воздействий на компоненты архивной системы
Класс 5. Источники угроз, связанные с деятельностью внутренних нарушителей	
Недобросовестное исполнение обязанностей	Сознательное неисполнение работниками определенных обязанностей или небрежное их исполнение
Халатность	Неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе
Причинение имущественного ущерба	Умышленное нанесение персоналом вреда информационным активам. В первую очередь вредительство может быть направлено на технические и программные средства, а также на информационные активы. Возможные последствия: ущерб, вызванный нарушением свойств активов, включая их разрушение и уничтожение
Ошибка персонала	Любые не соответствующие установленному регламенту или сложившимся практикам действия персонала, совершаемые без злого умысла. Возможные причины: недостаточно четко определенные обязанности, халатность, недостаточное обучение или квалификация персонала. Возникновению ошибок способствуют отсутствие дисциплинарного процесса и документирования процессов, предоставление избыточных полномочий, умышленное использование методов социального инжиниринга по отношению к персоналу. Возможные последствия: нарушение конфиденциальности и целостности информации, утрата информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов), сбои и отказы технических и программных средств
Хищение	Совершенное с корыстной целью противоправное безвозмездное изъятие и/или обращение имущества организации БС РФ, причинившие ущерб собственнику или иному владельцу этого имущества
Выполнение вредоносных программ	Внедрение в систему и выполнение вредоносных программ: программных закладок, троянских коней, программных вирусов и червей и т.п. Возможные причины: беспечность, халатность, низкая квалификация персонала (пользователей), наличие уязвимостей используемых программных средств. Возможные последствия: несанкционированный доступ к информационным активам, нарушение их свойств, сбои, отказы и уничтожение программных средств, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Использование информационных активов не по назначению	Умышленное использование информационных активов организации в целях, отличных от целей организации. Возможные причины: отсутствие контроля персонала. Возможные последствия: нехватка вычислительных, сете-

Источник угрозы	Описание
	вых или людских ресурсов, прямой ущерб организации
Нарушения персоналом организационных мер по обеспечению безопасности	Несоблюдение персоналом требований внутренних документов, регламентирующих деятельность по безопасности
Ошибки кадровой работы	Ошибки кадровой работы заключаются в приеме на работу неквалифицированных сотрудников, увольнении/перемещении сотрудников без проведения сопутствующих процедур по обеспечению ИБ, непроведении или нерегулярном проведении тренингов и проверок персонала
Класс 6. Источники угроз, связанные с деятельностью внешних нарушителей	
Действия неавторизованного субъекта	Умышленные действия со стороны субъекта из внешней по отношению к области обеспечения ИБ среды. Возможные последствия: разрушение и уничтожение технических и программных средств, внедрение и выполнение вредоносных программ, нарушение свойств, утрата информационных активов и сервисов
Ложное сообщение об угрозе	Ложное сообщение об угрозе, такой как: пожар, террористический акт, техногенная катастрофа, гражданские беспорядки и т.д. Возможные последствия: нарушение свойств информационных активов, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов)
Неконтролируемое уничтожение информационного актива	Неумышленное уничтожение информационных активов. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия: прямой ущерб организации
Неконтролируемая модификация информационного актива	Неумышленное изменение информационных активов. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия: нарушение непрерывности выполнения процессов, прямой ущерб организации
Несанкционированный логический доступ	Несанкционированный логический доступ неавторизованных субъектов к компонентам подразделения и информационным активам. Возможные причины: компрометация пароля, предоставление пользователям/администраторам избыточных прав доступа, недостатки (отсутствие) механизмов аутентификации пользователей и администраторов, ошибки администрирования, оставление без присмотра программно-технических средств. Одним из путей получения несанкционированного доступа к системе является умышленное внедрение вредоносных программ с целью хищения пароля для входа в систему или получения прав доступа. Возможные последствия: нарушение свойств информационных активов, сбои, отказы и аварии программных и технических средств, нарушение непрерывности процессов и/или снижение качества информационных услуг (сервисов)
Несанкционированный физический доступ	Физический несанкционированный доступ неавторизованных лиц в контролируемую зону расположения технических средств и/или информационных активов. Возмож-

Источник угрозы	Описание
	ные причины: может осуществляться путем обхода средств контроля физического доступа или использования утраченных/похищенных средств обеспечения доступа. Возможные последствия: разрушение и уничтожение технических и программных средств, нарушение конфиденциальности, целостности, доступности информационных активов, нарушение непрерывности процессов и/или снижение качества информационных услуг (сервисов)
Класс 7. Источники угроз, связанные с несоответствием требованиям надзорных и регулирующих органов, действующему законодательству	
Несоответствие внутренних документов действующему законодательству	Несоответствие деятельности может привести к административным и уголовным санкциям со стороны судебных, надзорных и регулирующих органов в отношении должностных лиц подразделения, вызвать остановку отдельных видов деятельности
Изменчивость и несогласованность требований надзорных и регулирующих органов, вышестоящих инстанций	Непостоянство, различия и коллизии в содержании требований и/или порядке их выполнения способны дезорганизовать деятельность подразделения или его отдельных служб, снизить ее эффективность и качество, а при определенных обстоятельствах – затруднить ее осуществление. Способствует «размыванию» или пересечению зон ответственности исполнителей и служб, манипуляции со стороны ответственных лиц и служб своими правами и обязанностями в ущерб общей деятельности. Приводит к перераспределению ресурсов в пользу той деятельности (зачастую не основной), за несоблюдение требований к которой наказание наиболее ощутимо для организации (должностного лица)

Уязвимости

Устранение или существенно ослабление уязвимостей, влияет на возможности реализации угроз

Существуют следующая классификация уязвимостей:

Объективные – зависят от особенностей построения и технических характеристик оборудования, применяемого в ИС. Полное устранение этих уязвимостей невозможно, они могут существенно ослабляться техническими и инженерно – техническими методами. К ним можно отнести:

1. Сопутствующие техническим средствам излучения:

– Электромагнитные (побочные излучения элементов технических средств, кабельных линий технических средств, излучения на частотах работы генераторов, на частотах самовозбуждения усилителей);

– Электрические (наводки электромагнитных излучений на линии и проводки, просачивание сигналов в сети электропитания, в цепи заземления, неравномерность потребления тока электропитания);

– Звуковые (акустические, виброакустические).

2. Активизируемые:

– Аппаратные закладки (устанавливаемые в телефонные линии, в сети электропитания, в помещениях, в технических средствах);

– Программные закладки (вредоносные программы, технологические выходы из программ, нелегальные копии ПО).

3. Определяемые особенностями элементов:

– Элементы, обладающие электроакустическими преобразованиями (телефонные аппараты, громкоговорители, микрофоны);

– Элементы подверженные воздействию электромагнитного поля (магнитные носители, микросхемы).

4. Определяемые особенностями защищаемого объекта:

– Местоположением объекта (отсутствие контролируемой зоны, наличие прямой видимости объектов, удаленных и мобильных элементов объекта);

– Организацией каналов обмена информацией (использование радиоканалов, глобальных информационных сетей, арендуемых каналов).

Субъективные – зависят от действий сотрудников, в основном устраняются организационными и программно-аппаратными методами:

1. Ошибки:

– При подготовке и использовании программно обеспечения (при разработке алгоритмов и программного обеспечения, инсталляции и загрузке программного обеспечения, эксплуатации программного обеспечения, вводе данных);

– При управлении сложными системами (при использовании возможностей самообучения систем, организация управления потоками обмена информации);

– При эксплуатации технических средств (при включении /выключении технических средств, использовании технических средств охраны, использование средств обмена информацией).

2. Нарушения:

– Режима охраны и защиты (доступа на объект, доступа к техническим средствам);

– Режима эксплуатации технических средств (энергообеспечения, жизнеобеспечения);

– Режима использования информации (обработка и обмен информацией, хранение и уничтожение носителей информации, уничтожения производственных отходов и брака);

– Режима конфиденциальности (сотрудники в не рабочее время, уволенные сотрудники; обиженные сотрудники).

Случайные – зависят от особенностей окружающей ИС среды и непредвиденных обстоятельств.

1. Сбои и отказы:

– Отказы и неисправности технических средств (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа);

– Старение и размагничивание носителей информации (дискет и съемных носителей, жестких дисков, микросхем, кабелей и соединительных линий);

– Сбои программного обеспечения (операционных систем и СУБД, прикладных программ, сервисных программ, антивирусных программ);

– Сбои электроснабжения (оборудования, обрабатывающего информацию; обеспечивающего и вспомогательного оборудования);

2. Повреждения:

– Жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации; кондиционирования и вентиляции);

– Ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий; корпусов технологического оборудования).

Задание

Произвести оценку угроз и уязвимостей критическим видам деятельности организации

Пример выполнения практической работы 5

Задание. Произвести оценку угроз и уязвимостей критическим видам деятельности организации

Все возможные угрозы деятельности компании «ПромАвтоматика»можно разделить на три основные группы:

Обусловленные действиями субъекта (антропогенные источники) – субъекты, действия которых могут привести к нарушению безопасности информации, данные действия могут быть квалифицированны как умышленные или случайные преступления. Источники, действия которых могут привести к нарушению безопасности информации могут быть как внешними так и внутренними. Данные источники можно спрогнозировать, и принять адекватные меры:

- потеря персонала;
- невыход персонала на работу;
- атаки хакеров;
- компьютерные вирусы;
- выход из строя обеспечивающих систем (халатность);
- угроза некорректности данных (ошибки персонала);
- угроза целостности данных (хищение).

Обусловленные техническими средствами (техногенные источники) – эти источники угроз менее прогнозируемы и напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности, также могут быть как внутренними, так и внешними:

- отказ компьютерных аппаратных средств;
- сбои в работе аппаратных и программных средств;
- выход из строя аппаратных средств.

Стихийные источники – данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия, или др. обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить), такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. Такие источники угроз совершенно не поддаются прогнозированию и, поэтому меры против них должны применяться всегда. Стихийные источники, как правило, являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы:

- пожары,
- наводнения,
- ураганы,
- землетрясения,
- нарушение функционирования систем жизнеобеспечения,
- нарушение внутриклиматических условий,
- нарушение электропитания и др.

Практическая работа 6.
Оценка воздействий и долговременных последствий отказов, отсутствия активов и ресурсов

Анализ характера и последствий отказов производится с использованием приоритетного коэффициента риска

$$Кр = Кп*Кн*Ко$$

который показывает, какие возможные отказы (и их причины) являются наиболее существенными (относительный приоритет отдельных отказов/причин), а, следовательно, по каким из них следует принимать предупреждающие меры в первую очередь. Анализ производится с использованием коэффициентов, принимающих во внимание все три указанные важнейшие факторы влияния на качество продукции. К этим коэффициентам относятся:

Кп – коэффициент, учитывающий значение последствий отказов (тяжесть последствий проявления причин отказов) для потребителя (см. табл. 1). Потребителем всегда является конечный потребитель (покупатель). При анализе процесса потребителем считают того, кто принимает результат предыдущего этапа (и, в конце концов, конечного потребителя).

Кн – коэффициент, учитывающий вероятность Рн, с которой отказ или его причина не могут быть обнаружены до возникновения последствий непосредственно у потребителя (см. табл. 2). Нужно отметить, что вероятность пропуска (необнаружения) причины численно равна среднему выходному уровню дефектности.

Ко – коэффициент, учитывающий вероятность Ро отказа. Обычно

$$Ро=1 - Рб,$$

где Рб – вероятность отсутствия отказа (табл. 3 или, если вероятность отказа выражена в ppm). При определении Ро исходят из того, что отказ не обнаружится до тех пор, пока потребитель не начнет пользоваться изделием.

Таблица 1

Коэффициент Кп, учитывающий значение последствий отказов для заказчика (внутреннего/внешнего)

Значение последствий отказа	Показатель
Вероятность, близкая к нулю, что дефект может иметь какие - либо ощутимые последствия. Видимое воздействие на функцию или на дальнейшее выполнение операций процесса невозможно	1
Незначительное влияние на функции системы или дальнейшее выполнение операций процесса (второстепенное несоответствие). Потребитель, вероятно, заметит лишь незначительную неисправность системы.	2-3
Умеренное влияние. Вызывает недовольство потребителя. Функции системы или дальнейшему выполнению операций процесса нанесен ущерб (значительное несоответствие).	4-6
Существенное влияние. Существенные функции системы полностью выпадают, или промежуточный продукт не поддается дальнейшей обработке (значительное несоответствие). Несоответствие вызывает досаду потребителю, но безопасность или соответствие законам здесь не затрагиваются.	7-8
Очень существенное влияние. Тяжелые последствия отказа, ведущие к остановке производства.	9
Критическое. Отказ угрожает безопасности (опасность для жизни и здоровья людей) и противоречит законодательным предписаниям.	10

Таблица 2

Коэффициент Кн, учитывающий вероятность Рн, невыявления отказа или его причины

Значение последствий отказа	Вероятность невыявлениярн %	Показатель
Близкая к нулю. Возникающие отказы или причины отказов явно распознаются (например, отсутствие отверстия для сборки)	не более 0,01	1
Очень маленькая. Выявление возникающих отказов или причин отказов очень вероятно, например, с помощью большого количества независимых друг от друга испытаний/ технологических проверок (автоматический сортировочный контроль одного признака)	не более 0,01	2-3
Небольшая. Выявление возникающих отказов или причин отказов вероятно; проводимые испытания/ технологические проверки относительно достоверны	не более 0,3	4-5
Умеренная. Выявление возникающих отказов или причин отказов менее вероятно; проводимые испытания/ технологические проверки недостаточно достоверны (традиционный контроль - выборочный контроль, эксперименты, тесты)	не более 2	6-7
Высокая. Выявление возникающих отказов или причин отказов весьма затруднительно; проводимые испытания / технологические проверки очень неэффективны (например, контроль ручным способом, т.е. зависимость от персонала; признак распознается с трудом - неправильно выбран материал)	не более 10	8-9
Очень высокая. Возникающие отказы или причины отказов выявить нельзя: технологические проверки не проводятся (например: нет доступа, нет возможности для контроля, срок службы)	более 10	10

Таблица 3

Коэффициент Ко, учитывающий вероятность Ро возникновения причины отказа

Значение последствий отказа	Вероятность отказов/ дефектов Ро %	Показатель
Вероятность близка к нулю	менее 0,00001	1
Очень незначительная вероятностью. Конструкция в общем соответствует прежним проектам, при применении которых наблюдалось сравнительно незначительное количество отказов. Процесс статистически стабилен при Ср (и Срк)=1-1,3. Доля дефектов при контроле качества составляет	0,00001 <Ро<Д0005	2-3
Незначительная вероятность. Конструкция в общем соответствует проектам, применение которых привело к появлению небольшого числа отказов. Технология сопоставима спрежней, при которой в незначительном объеме появляются дефекты. При коэффициенте Ср более, чем 0,85 доля дефектов в пределах	0,0005<Ро.< 0,5	4-6
Средняя вероятность. Конструкция в общем соответствует проектам, применение которых в прошлом всегда вызывало трудности. Процесс сопоставим с прежним, который часто приводил к дефектам	0,5<Ро<5	7-8
Высокая вероятность. Конструкция - ненадежна. Требования к проекту учтены незначительно (менее	Рп>5	9-10

Окончание табл. 3

Значение последствий отказа	Вероятность отказов/ дефектов Ро %	Показатель
50%). Процесс – нестабилен. Можно почти с уверенностью сказать, что дефекты появятся в значительном количестве		

Каждый из этих трех коэффициентов может иметь числовые значения в пределах от 1 до 10, поэтому коэффициент риска Кр колеблется от 1 до 1000. Следует обращать внимание на устранение тех причин, которые характеризуются наибольшими значениями коэффициента риска. Обычно считают опасными причины при Кр > Крп=100 (150), (где Крп – принятое на предприятии предельное значение Кр). Однако нужно также иметь в виду, что часто оценка бывает субъективна, и вывод о необходимости только, чтобы было Кр>Крп дезориентирует. Некоторые фирмы (например, немецкая фирма BOSCH) считают, что если хотя бы один из коэффициентов Ко, Кн или Кт имеет значение равное 10, то при любом значении обобщенного коэффициента риска Кр следует проводить анализ FMEA. Правильным может быть только подход, при котором все приведенные причины дефектов проверяются на возможность проведения мероприятий по их устранению. При этом в связи с затратами ориентируются на убывающую величину Кр, т.е. Кр устанавливает приоритет последовательности необходимых мероприятий.

Важнейшим этапом анализа характера и последствий отказа является проведение целенаправленных мероприятий по предупреждению дефектов. Эти мероприятия должны вести к одному из следующих результатов;

– избежанию причин отказов;

– снижению вероятности появления отказа (что возможно вследствие изменения конструкции или процесса, например, включение в конструкцию запасных параллельных элементов, выбор другого материала или термообработки);

– снижению влияния первопричины на появление отказа и тяжесть его последствий (что возможно благодаря изменению конструкции, например, снижение вибраций по отношению к предельному уровню возможно при включении упругого элемента в трансмиссию машины, что позволяет в несколько раз уменьшить динамические нагрузки);

– повышению вероятности обнаружения отказа на предприятии до момента поставки продукции потребителю (обычно это достигается изменением конструкции и процесса, а также в результате совершенствования мероприятий по обнаружению дефектов).

Задание

Произвести оценку воздействий и долговременных последствий отказов, отсутствия активов и ресурсов

Пример выполнения практической работы 6

Задание. Произвести оценку воздействий и долговременных последствий отказов, отсутствия активов и ресурсов

Показатели расчета приоритетного коэффициента риска

Бизнес-процесс	Коэффициент риска
Реализация АИС	8*5*4=160
Разработка ПС в соответствии с ТЗ	8*6*8=384
Выполнение работ в соответствии с гарантийными обязательствами	6*6*7=252
Удержание имеющихся клиентов	8*5*8=320
Организация работы компьютерной инфраструктуры	8*5*3=120
Поиск новых клиентов	6*4*5=144
Ведение бухгалтерской отчетности	8*4*6=192
Начисление заработной платы	9*4*6=216

Наибольшие значения по расчетам были оценены процессы – Разработка ПС в соответствии с ТЗ (384), Удержание имеющихся клиентов (320), Выполнение работ в соответствии с гарантийными обязательствами (252).

Важнейшим этапом анализа характера и последствий отказа является проведение целенаправленных мероприятий по предупреждению дефектов. Эти мероприятия должны вести к одному из следующих результатов:

– избежанию причин отказов;

– снижению вероятности появления отказа;

– снижению влияния первопричины на появление отказа и тяжесть его последствий;

– повышению вероятности обнаружения отказа на предприятии до момента поставки продукции потребителю.

Практическая работа 7.
Стратегия управления непрерывностью бизнеса

После того как мы разобрались, что угрожает критичным бизнес-процессам организации, необходимо определить как будет обеспечиваться непрерывность бизнеса.

Цель и область применения

Целью документа является восстановление критичных важных организационных и технических процессов после их сбоя, определив четкую последовательность действий.

Обеспечение непрерывности бизнеса включает в себя такие цели:

– поддержание способности компании выполнять принятые на себя обязательства перед клиентами и партнерами, предупреждение и предотвращение возможного нарушения режима повседневного функционирования компании;

– сохранение уровня управления компании, позволяющего обеспечить условия для принятия обоснованных и оптимальных управленческих решений, своевременную полную реализацию;

– снижение последствий нарушения режима повседневного функционирования;

– обеспечение соответствия всех механизмов принципов непрерывности бизнеса требованиям нормативно-правовых актов, государственных стандартов, утвержденных в компании актов, планов, программ и т.п.

Основным приоритетом безопасности работы организации являются люди, т.е. должны быть инструкции, направленные на обеспечение здоровья до, во время и после прерывания бизнеса. Относительно защиты активов, предусматривается две концепции:

– усиление за счет использования различных защитных мер и средств;

– дублирование.

В процессе выбора решения необходимо детально рассмотреть возможные действия в отношении помещений, технологий, информационных активов, контрагентов, а также партнеров. Данные решения, как правило, выбираются с целью:

– защиты приоритетных видов деятельности компании;

– их эффективного восстановления;

– смягчения последствий инцидентов, разработки ответных и превентивных мер.

В качестве дублирования информационной системы используется концепция альтернативных площадок, к которым относят, главным образом, следующие:

– площадка в горячем резерве (Hot Site), когда альтернативная площадка максимально соответствует реальной (т.е. обеспечивается режим готовности 24/7);

– площадка в теплом резерве (Warm Site), когда на альтернативной площадке развернут прототип реальной компьютерной системы, например, в нали-

чии все коммуникации и базовые устройства, однако информационные базы не актуализированы, отдельные настройки и обновления не произведены и т.п.;

– площадка в холодном резерве (Cold Side) – как правило, это лишь помещение;

Надо понимать, что, кроме увеличения затрат при снижении времени аварийного восстановления, наиболее актуализированные площадки требуют обеспечения и соответствующего уровня безопасности.

В качестве особых мер защиты еще выделяют:

– «джентльменское» соглашение о взаимопомощи с другими организациями (reciprocal or mutual aide agreement);

– аутсорсинг – на договорной основе использование подрядчиков (service bureaus).

В качестве стратегий актуализации данных с альтернативными площадками можно назвать следующие:

– копирование резервных данных (electronic vaulting, off-site data protection) – периодическая передача копий баз данных на альтернативные носители, обычно в пакетном режиме;

– удаленное журналирование (remote journaling) – периодическая передача журнала выполненных транзакций с основной площадки на альтернативную;

– удаленное зеркалирование (remote mirroring) – полное дублирование в реальном времени.

Известно несколько схем резервного копирования, например:

– полное копирование (full backup), когда копируются все файлы или блоки;

– инкрементальное или добавочное копирование (incremental backup), когда копируются только измененные файлы или блоки после последнего (инкрементального или полного) копирования;

– дифференциальное копирование (differential backup), когда копируются все измененные файлы или блоки с момента последнего полного копирования.

Задание

Используя ГОСТ Р 53647.1-2009 Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство определите стратегию непрерывности бизнеса своей организации

Пример выполнения практической работы 7

Задание. Используя ГОСТ Р 53647.1-2009 Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство определите стратегию непрерывности бизнеса своей организации

Настоящая стратегия описывает метод построения процессов обеспечения непрерывности бизнес-процессов ЗАО «ПромАвтоматика» и определяет базовую совокупность правил, требований и руководящих принципов, направленных на:

– организацию оценки критичности бизнес-процессов ИТ-компании;

– обеспечение непрерывности критичных бизнес-процессов ИТ-компании;

– минимизацию ущерба, наносимого деятельности ИТ-компании возникновением чрезвычайных ситуаций;

– обеспечение соответствия мер, принимаемых в области обеспечения непрерывности бизнеса ИТ-компании;

– предоставление работникам рекомендаций и содействия в области обеспечения непрерывности бизнеса.

Данный документ должен рассматриваться строго в соответствии с другими внутренними документами ЗАО «ПромАвтоматика». В случае возникновения противоречий между данным документом и другими внутренними документами, затрагивающими вопросы политики обеспечения непрерывности бизнеса, данный документ имеет более высокий приоритет в части процессов обеспечения непрерывности бизнеса.

Основными целями ОНБ являются:

– поддержание способности бизнес-процессов ЗАО «ПромАвтоматика» выполнять принятые на себя функции, предупреждение и предотвращение возможного нарушения режима повседневного функционирования отдела;

– снижение тяжести последствий нарушения режима повседневного функционирования ЗАО «ПромАвтоматика» (в том числе размера потерь информации);

– сохранение уровня управления ЗАО «ПромАвтоматика», позволяющего обеспечить условия для принятия обоснованных и оптимальных управленческих решений, их своевременную и полную реализацию;

– обеспечение благоприятных условий труда и безопасности сотрудников, безопасности посетителей, находящихся в кабинетах ЗАО «ПромАвтоматика»;

– определение перечня Критичных процессов ЗАО «ПромАвтоматика» и перечня сценариев негативного развития событий, способных привести к остановке бизнес-процессов;

– обеспечение непрерывности деятельности критичных бизнес-процессов ЗАО «ПромАвтоматика» за счет определения, внедрения и документирования механизмов контроля, включая План(ы) ОНиВД разработанные для каждого структурного подразделения и/или рабочей группы.

– Каждый План ОНиВД описывает потребности структурной единицы в ресурсах, необходимых для реализации плана в части продолжения и восстановления деятельности от момента объявления ЧС до ее завершения и переход в режим повседневного функционирования.

Стратегия ОНБ включает в себя:

– определение областей, в рамках которых организация может быть подвержена рискам непрерывности;

– определение рисков, которые могут повлиять на функционирование отдела;

– рассмотрение и анализ риска возникновения природных, техногенных катастроф, равно, как и других непредвиденных обстоятельств, применимых к ЗАО «ПромАвтоматика»;

– рассмотрение рисков, реализация которых наносит существенный ущерб материальным и нематериальным активам диспетчерской;

– анализ факторов, влияющих на вероятность наступления ЧС;

– анализ степени влияния ЧС на сотрудников;

– инфраструктуру ЗАО «ПромАвтоматика»;

– информационные активы ЗАО «ПромАвтоматика».

Цель настоящего документа – в случае сбоев в работе критически важных сервисов обеспечить их восстановление на резервном оборудовании, определив четкую последовательность действий, которые должны выполнить сотрудники компании.

К важным сервисам относятся:

– электронная почта;

– файловый сервис.

Переход на сервера холодного резерва в случае аварийной ситуации

Сервис электронной почты

Основным принципом восстановления работоспособности сервиса электронной почты является создание кластера и установка ПО на резервной площадке с точно такими же адресами, именами, версией, и почтовыми базами, как и на основной. Кластер на основной площадке должен быть обязательно выключен.

Для восстановления необходимо выполнить следующие шаги.

1. Кластер в основной серверной должен быть выключен.

Так как имя восстанавливаемого сервиса, адресация и другие параметры будут иметь точно такое же значение, необходимо удостовериться, что сервера, входящие в кластер выключены.

2. Сбросить пароль учетной записи сервера

Выполните вход на рабочей станции или сервере, имеющей права доменного администратора.

3. Переименовать резервный сервер, задать то имя, которое установлено на штатном сервере.

4. Настроить адресацию на резервном сервере.

Открыть окно сетевых подключений. Выбрать интерфейс. Открыть свойства TCP/IP. Присвоить необходимые параметры.

5. Вести резервный сервер в домен.

6. Проверить принадлежность к домену утилитной командной строки nltest.

7. Восстановить базы почтовых ящиков на хранилище.

8. Установить кластер.

Создать новый кластер с параметрами старого.

Файловый сервер

Для обеспечения «холодного» резерва используется встроенная служба Microsoft Windows 2003 Server – Distributed File System (DFS).

DFS – один из инструментов Active Directory. Он позволяет создавать сетевые ресурсы, в которые могут входить множество файловых систем на различных машинах. Для пользователя Active Directory это абсолютно прозрачно и не имеет никакого значения, где и на каких машинах физически расположены те файлы, с которыми он работает – для него они все лежат в одном месте. Кроме этого, при использовании DFS и Active Directory упрощается управление такими ресурсами. Оно централизовано, можно просто и безболезненно добавлять новые ресурсы или удалять старые, менять физическое месторасположение файлов, входящих в DFS и т.д.

На резервной площадке установлен файловый сервер, который хранит реплику основных файловых ресурсов организации. В случае аварийной ситуации пользователи в ручном режиме переключаются на резервный сервер.

Проект репликации DFS.

В стандартной установке Windows Server без DFS операционная система обычно хранит пользовательские файлы в папках на сервере, и эти папки являются папками общего доступа для конечных пользователей Для того чтобы работать с файлами в папках общего доступа, конечные пользователи подключаются к этим сетевым ресурсам или непосредственно, или с помощью назначения букв для сетевых дисков. Подключение к сетевым ресурсам упрощает поиск данных в сети для конечных пользователей и состоит из четырех функциональных уровней, начиная с уровня пользователя и его ресурса, затем идет уровень папки, уровень файла и, наконец, уровень физического диска. В зависимости от того, как планируется проектировать инфраструктуру DFS, возможно, понадобится один или два дополнительных уровня – обязательный уровень корня DFS и необязательный уровень связей DFS.

Корневой уровень Dfs подобен корню жесткого диска – у каждого диска должен быть корень, и структура Dfs не исключение. Когда создается структура Dfs, следует выделить один или несколько ресурсов сети, которые будут выступать в роли корня Dfs. Чтобы иметь некоторый запас, можно создать корневые ресурсы на нескольких серверах в рамках одной структуры Dfs.

В Windows Server процесс создания корня Dfs начинается с запуска оснастки Microsoft Management Console (MMC) Distributed File System через Start, Programs, Administrative Tools. Следует щелкнуть правой кнопкой по Distributed File System в правой панели оснастки, затем выбрать New Dfs Root, чтобы запустить мастер конфи-

гурации. Поскольку мы определяем корень Dfs для поддержки репликации между узлами, нам необходим доменный корень Dfs.

После выбора домена следует определить главный сервер для корня Dfs, затем выбрать общий ресурс, который будет использоваться в дальнейшем. Если ресурс не был создан в самом начале, можно сделать это позже. Ресурс должен быть привязан к папке на диске NTFS, поскольку FRS использует систему протоколирования NTFS 5.0 (NTFS 5) для отслеживания момента изменения файла.

Заключительный шаг в конфигурации корня Dfs – присвоение ему имени. Подобно имени домена, пользователи будут задействовать это имя корня Dfs, чтобы подключиться к структуре Dfs. Имя корня Dfs – SyncFiles.

По завершении этого шага тестируем новый корень Dfs с какой-нибудь рабочей станции, подключаясь к UNC-имени <*domainname**Dfsrootname*>, которое было определено в процессе создания корня Dfs (promavt.org\SyncFiles). Рабочая станция извлечет данные Dfs из AD, а затем найдет лежащие ниже корня общие ресурсы.

План аварийного восстановления сервисов ЗАО «ПромАвтоматика»

Добавление избыточности в Dfs

На данном этапе у нас есть структура корня Dfs, но корень не продублирован. Поэтому следующий шаг – создание реплики корня Dfs нажатием правой кнопки мыши Distributed File System в левой панели оснастки Distributed File System. Необходимо выбрать в контекстном меню пункт New Root Replica, чтобы запустить мастер Dfs Root Wizard. Сначала следует выбрать компьютер, который планируется назначить главным компьютером для копии корня Dfs (ahk-fs-01). Затем нужно выбрать общий ресурс, который был определен перед запуском мастера – promavt-dfsroot.

После того как указан общий ресурс для корня Dfs на втором сервере, следует выполнить настройку репликации между обоими ресурсами. По умолчанию Dfs не настраивает репликацию данных автоматически, поэтому ее придется включить. Нужно щелкнуть правой кнопкой по созданному корню Dfs, затем выбрать Replication Policy из контекстного меню, чтобы открыть диалоговое окно Replication Policy. Следует щелкнуть Enable, чтобы включить репликацию для каждого ресурса, а затем определить, какой ресурс будет главным во время первой репликации. Выберите Set Master для этого ресурса. После выполнения перечисленных шагов Windows 2000 будет реплицировать данные между этими ресурсами и содержать их синхронизированными. Как только произойдет первоначальная репликация, разница между первичным ресурсом и другими ресурсами исчезнет.

Следующим шагом определяем список каталогов и подкаталогов для добавления в корень Dfs. Windows Server будет автоматически синхронизировать данные между всеми ресурсами корня Dfs. Все критически важные файлы данных располагаем внутри структуры Dfs. В случае аварийной ситуации информация будет реплицирована и доступна на других площадках организации.

Окончание настройки репликации Dfs для конкретной среды зависит от того, как предполагается реализовать Dfs. В данный момент уже можно переносить каталоги, подкаталоги и файлы в корень Dfs, а Windows 2000 будет автоматически синхронизировать данные между всеми ресурсами корня Dfs. Точнее

говоря, можно целиком задействовать древовидную структуру каталогов, чтобы все критически важные файлы данных располагались где-нибудь внутри структуры Dfs. Тогда можно быть уверенным, что в случае глобального сбоя (катастрофы) эта информация будет реплицирована и доступна из других офисов организации.

Можно пойти еще дальше и создать ссылки Dfs внутри структуры Dfs. Ссылки Dfs появляются перед конечными пользователями как папки в рамках структуры Dfs, но реально они представляют собой новые ресурсы, определенные внутри структуры Dfs. Ссылки Dfs особенно полезны, когда имеются различные типы данных, которые уже существуют на нескольких серверах, и требуется консолидировать эту информацию в единую структуру каталогов с простой навигацией. Для того чтобы создать ссылку Dfs, нужно щелкнуть правой кнопкой по вновь определенному корню Dfs в левой панели оснастки Distributed File System, затем выбрать New Dfs Link для запуска мастера конфигурации. Как и при конфигурации корня Dfs, мастер попросит выбрать серверы и ресурсы, которые будут участвовать в связи, и установить репликацию между ресурсами.

Общее время восстановления не должно превышать 30 минут.

Переход на основные сервера при возвращении в штатный режим работы системы

Процедура перехода на сервера основной серверной осуществляется в нерабочее время, когда остановка критических служб не влияет на бизнес-процессы организации.

Сервис электронной почты

Создание актуальной резервной копии почтовых ящиков.

Перед обратным переходом на сервера, расположенные в основной серверной необходимо создать на основном хранилище актуальную копию почтовых баз с резервного сервера. Для этого необходимо остановить хранилище и скопировать содержимое диска, где хранятся базы почтовых ящиков на файловый ресурс соответствующего объема. Выключить резервный кластер. Необходимо помнить, что кластер в основной серверной на данном этапе выключен.

Запуск кластера в основной серверной.

Включить узел основного кластер. Временно отключить хранилище. Скопировать актуальную резервную копию баз почтовых ящиков с файлового ресурса. Сбросить пароль учетной записи. Переподключить в домен сервер из основной серверной.

Файловый сервис

Для резервирования файлового сервиса используется Dfs. При восстановлении файлового сервиса необходимо убедиться, что выполнена синхронизация реплики между резервной и основной площадкой.

Практическая работа 8
Разработка организационно-распорядительной документации

Основой создания любой системы менеджмента является документирование. На схеме представлен возможный вариант структуры организационно-распорядительных документов в области непрерывности бизнеса (рис. 11).

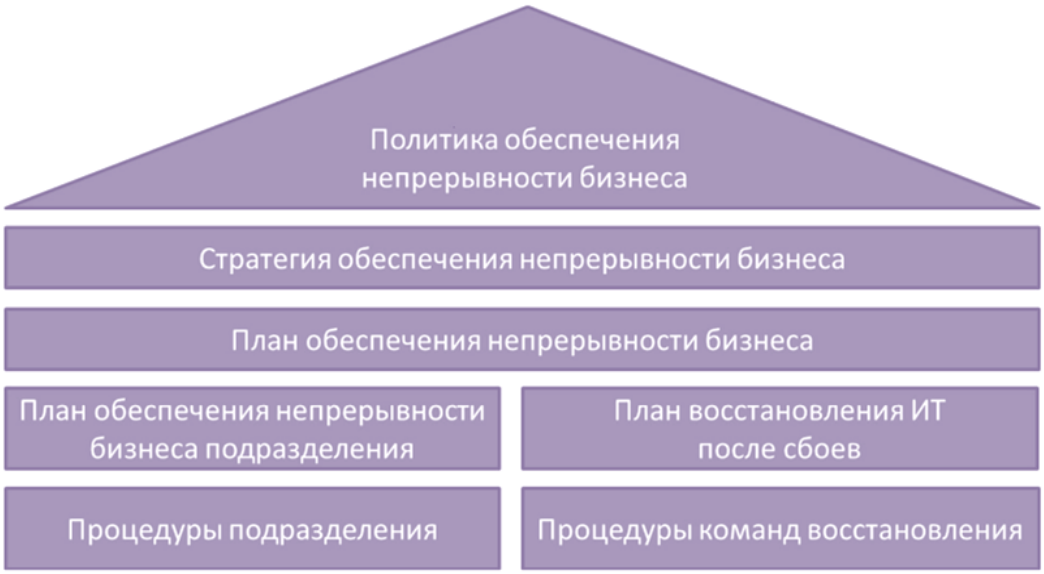

Рис. 11. Структура организационно-распорядительных документов в области непрерывности бизнеса

Самым высокоуровневым документом является Политика обеспечения непрерывности бизнеса (Business continuity policy statement), которая содержит основные цели, задачи и принципы в области обеспечения непрерывности бизнеса. Иногда в качестве приложения к Политике безопасности создают документ Стратегия обеспечения непрерывности бизнеса (Business continuity strategy). Следует заметить, что вся деятельность по управлению непрерывности бизнеса начинается с одобрения руководством путем утверждения указанной политики.

План обеспечения непрерывности бизнеса (Business continuity plan) – общий план, описывающий систему менеджмента обеспечения непрерывности бизнеса. Зачастую является неким подобием руководства по качеству только для рассматриваемых нами целей.

План обеспечения непрерывности бизнеса подразделения (Business unit continuity plan) – план действий сотрудников определенного подразделения в кризисной ситуации.

Процедуры по обеспечению непрерывности бизнеса подразделения (Business unit continuity procedures) – описание конкретных процедур подразделения, которые в случае необходимости можно вынести их из плана подразделения (например, PR-подразделению в кризисной ситуации необходимы отдельные процедуры для организации внутренних и внешних коммуникаций).

План восстановления ИТ-системы после сбоев (IT disaster recovery plan) – план восстановления информационных систем и ИТ-инфраструктуры предприятия. Ключевыми составляющими плана являются описание зависимостей систем и последовательности их восстановления.

Процедуры команд восстановления (Emergency team procedures) – процедуры команд восстановления.

План – это заранее намеченная система мероприятий, предусматривающая порядок, последовательность и сроки выполнения работ.

В соответствии с лучшими практиками ISO 22301 Societal security – Business continuity management systems – Requirements, ГОСТ Р 53647 «Менеджмент непрерывности бизнеса», NIST Special Publication 800-34 Rev. 1 «Contingency Planning Guide for Federal Information Systems», планы управления непрерывностью должны состоять из трёх компонентов:

1. Реагирование на чрезвычайные ситуации – определяет последовательность действий, которые необходимо осуществить при обнаружении инцидента.

2. Управление инцидентами – определяет методы, необходимые для смягчения или уменьшения размера происшествия.

3. Восстановление деятельности – определяет последовательность действий, которые необходимо осуществить для того, чтобы восстановить сервис на заданном уровне.

В планах BCP должны быть рассмотрены:

- первоначальные шаги по реагированию на любые кризисные события (когда еще неизвестно, какую конкретно процедуру плана BCP нужно будет запускать); обычно это сбор ключевых сотрудников (команды BCP), информирование руководства и др.
- критерии активации и деактивации плана;
- детальные процедуры по восстановлению для каждого из кризисных событий; можно разместить их в виде приложений к плану;
- критерии успешности процедуры восстановления;
- процедура тестирования плана BCP;
- полезные контакты, практики, ссылки и т.д.

Примерная структура плана обеспечения непрерывности бизнеса:

1. Введение
   1.1. Исходная информация
   1.2. Границы действия плана
   1.3. Предпосылки создания плана
2.Концепция
   2.1.Описание системы обеспечения непрерывности
   2.2.Описание этапов восстановления непрерывности
   2.3.Роли и их обязанности
3.Активация плана
   3.1.Критерии и порядок активации

3.2.Порядок уведомления заинтересованных лиц
3.3.Порядок оценки происшествия
4.Контроль
5.Восстановление
5.1.Последовательность восстановления непрерывности

Специалистами NIST было разработано руководство, которое достаточно подробно описывает необходимые) планы обеспечения непрерывности бизнеса. Далее приведена таблица, где описан каждый из планов (указанных в руководстве NIST), а также даны ссылки на стандарты / нормативно-правовые акты, которые предписывают разработку таких планов.

Наименование плана	Описание плана	Стандарт/ НПА
Business Continuity Plan (BCP) План обеспечения непрерывности бизнеса	Набор задокументированных процедур, которые разработаны, обобщены и актуализированы с целью их использования в случае возникновения инцидента, и направлены на обеспечение возможности продолжения выполнения компанией критических важных видов деятельности на установленном приемлемом уровне.	ISO 22301 «Социальная безопасность. Системы менеджмента непрерывности бизнеса»: 8.4.4 Планы непрерывности бизнеса (Business continuity plans)
Continuity of Operations Plan (COOP) План непрерывность операций	Фокусируется на восстановлении критически важных функций компании на альтернативной площадке и на их выполнении в течение 30 дней.	-
Crisis Communication Plan План антикризисных коммуникаций	В данном плане задокументированы процедуры и правила внешних и внутренних коммуникаций в случае чрезвычайных ситуаций.	Федеральный закон от 21.12.1994 № 68 «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»: Статья 14. Обязанности организаций в области защиты населения и территорий от чрезвычайных ситуаций (*«Организации обязаны предоставлять в установленном порядке информацию в области защиты населения и территорий от чрезвычайных ситуаций, а также оповещать работников организаций об угрозе возникновения или о возникновении чрезвычайных ситуаций*»).
Critical Infrastructure Protection Plan (CIP) План защиты критических инфраструктур	План направлен на защиту ключевых ресурсов и компонентов национальной инфраструктуры.	Указ Президента Российской Федерации от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».
Cyber Incident Response Plan План реагирования на кибер-инциденты	План, описывающий процедуры реакции на инциденты, связанные с атаками хакеров, вторжения в информационную систему и другие проблемы безопасности.	ГОСТ Р ИСО/МЭК ТО 18044—2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»;

Наименование плана	Описание плана	Стандарт/ НПА
		NIST 800-61 «Computer Security. Incident Handling Guide».
Disaster Recovery Plan (DRP) План восстановления после сбоя	План восстановления инфраструктуры компании после возникновения аварии.	ISO 22301 «Социальная безопасность. Системы менеджмента непрерывности бизнеса»: 8.4.5 Восстановление (Recovery).
Information System Contingency Plan (ISCP) План на случай непредвиденных ситуаций в информационных системах	План восстановления системы, сетей и основных приложений после аварии. Данный план необходимо разработать для каждой критической системы и/или приложения.	-
Occupant Emergency Plan (OEP) План действия персонала в случае чрезвычайной ситуации	В данном плане определяется порядок обеспечения безопасности персонала и процедуры эвакуации в случае чрезвычайных ситуаций.	Федеральный закон от 21.12.1994 г. № 68 «О защите населения и территории от чрезвычайных ситуаций природного и техногенного характера»; Федеральный закон от 21.12.1994 № 69 «О пожарной безопасности».

Вышеперечисленные документы составляются исходя из потребностей компании, но на практике чаще всего применяются следующие виды планов:

– План реагирования на инциденты – данный вид плана может включать в себя план реагирования на кибер-инциденты, план на случай непредвиденных ситуаций в информационных системах. Данный план поможет уменьшить масштабы катастрофы и смягчить ее последствия, что даст возможность сэкономить время и дополнительное преимущество при активации остальных типов планов;

– План действия персонала в чрезвычайных ситуациях – в соответствии с требованиями Федерального закона от 21.12.1994 г. №68 68 «О защите населения и территории от чрезвычайных ситуаций природного и техногенного характера» и Федерального закона от 21.12.1994 г. №69 «О пожарной безопасности» этот план является обязательным для всех компаний;

– План восстановления после сбоя – сфокусирован на восстановлении критически важных информационных систем. Данный вид плана осуществляет поддержу плана обеспечения непрерывности бизнеса и направлен на восстановление работоспособности отдельных систем и приложений;

– План обеспечения непрерывности бизнеса – сфокусирован на поддержке бизнес-процессов компании во время и после чрезвычайной ситуации; направлен на обеспечение возможности продолжения выполнения компанией критических важных для нее видов деятельности на установленном приемлемом уровне;

– План антикризисных коммуникаций – данный план поможет сохранить репутацию компании в кризисной ситуации. В нем документируется порядок взаимодействия со СМИ, правоохранительными органами, МЧС и т.д.

Обслуживание и обновление планов

Как уже отмечалось выше, управление непрерывностью бизнеса компании является циклическим процессом. А это значит, что нельзя ограничиваться одним только формированием планов, необходимо сопровождать, обновлять и совершенствовать их ежегодно, а иногда и чаще, например, в следующих случаях:

1. Изменение ИТ-инфраструктуры;
2. Изменение организационной структуры компании;
3. Изменения в законодательстве;
4. Обнаружение недостатков в планах при их тестировании.

Чтобы сохранить актуальность планов, необходимо выполнять следующие действия:

- проводить внутренние аудиты, включающие проверку восстановления после аварий, документации по обеспечению непрерывности и соответствующих процедур;
- проводить регулярные практические тренинги по выполнению плана;
- интегрировать вопросы непрерывности бизнеса в процесс управления изменениями компании.

Задание

Разработайте План обеспечения непрерывности бизнеса своей организации

Пример выполнения практической работы 8

Задание. Разработайте План обеспечения непрерывности бизнеса своей организации

Цель и область применения

Целью документа является восстановление критичных важных организационных и технических процессов после их сбоя, определив четкую последовательность действий.

Обеспечение непрерывности бизнеса включает в себя такие цели:

– поддержание способности компании выполнять принятые на себя обязательства перед клиентами и партнерами, предупреждение и предотвращение возможного нарушения режима повседневного функционирования компании;

– сохранения уровня управления компании, позволяющего обеспечить условия для принятия обоснованных и оптимальных управленческих решений, своевременную полную реализацию;

– снижение последствий нарушения режима повседневного функционирования;

– обеспечение соответствия всех механизмов принципов непрерывности бизнеса требованиям нормативно-правовых актов, государственных стандартов, утвержденных в компании актов, планов, программ и т.п.

План обеспечения непрерывности включает поддержку процесса восстановления в штатный режим работы следующих сервисов: электронная почта, файловый сервис.

Рамки плана.

Настоящий план предназначен для случаев сбоев в работе критически важных сервисов, вызванных сбоями оборудования/программного обеспечения (аварийный режим) более чем на 2 часа. План предназначен для использования в случае:

– с неблагоприятными событиями природного, техногенного и социального характера (пожар, чрезвычайные ситуации и стихийные бедствия, техногенные катастрофы, нарушение электропитания, нарушение функционирования жизнеобеспечения);

– серьезных инцидентов в области информационной безопасности (вирусные атаки, DOS атаки, приводящие к нарушению работоспособности всех информационных систем, социальный инжиниринг, ошибки персонала, недобросовестное исполнение обязанностей, использование информационных активов не по назначению, несанкционированный доступ).

– связанные со сбоями, отказами, разрушениями/повреждениями программных и технических средств (выхода из строя аппаратных компонентов, выхода из строя оборудования кондиционирования в серверном помещении, сбои и отказы программных средств, нарушения функциональности криптографической системы, нарушения функциональности архивной системы).

Распределение функций, ответственности и полномочий

Для поддержания готовности к реагированию при реализации угроз, влияющих на непрерывность сервиса, необходимо создание восстановительной команды:

- руководитель АВК;
- координатор планирования обеспечения непрерывности;
- ответственный за резервное копирование;
- ответственный за выделение рабочих площадок;
- ответственный за функционирование локальной сети;
- ответственный за функционирование каналов передачи данных;
- ответственный за резерв аппаратного обеспечения;
- администратор;
- специалист технической поддержки пользователей.

Целевые параметры восстановления

Задачей плана является восстановление сервис в течение 1-3 ч. На восстановление каждого сервиса отводится 1 час.

Допустимой потерей данных при восстановлении системы является потеря данных за интервал в 2 ч.

Стратегия выполнения

Общей стратегией выполнения плана является:

- оповещение ответственного администратора;
- диагностика неисправности;
- переход работы сервисов на оборудование «холодного» резерва;
- работа на оборудовании «холодного» резерва;
- восстановление штатного способа предоставления сервиса;
- возврат к штатному режиму функционирования.

Активация плана

Активация настоящего плана производится: визуальный осмотр серверного помещения и определение невозможности запуска аппаратных средств, получение информации от энергокомпании о выключении электропитания в серверном помещении более чем на 2 часа, выход из строя аппаратных компонентов и невозможности их замены.

В случае наступления данного события, ответственный администратор системы должен быть незамедлительно уведомлен о необходимости активации плана.

Активацию данного плана не следует проводить в случаях: кратковременного (до 2 часов) выключения электропитания, проведения монтажных и других работ в серверном помещении, связанных с отключением электропитания в серверном помещении.

Актуализация плана

Настоящий план подлежит пересмотру каждые 6 месяцев. В рамках процедуры актуализации плана должна быть проверена актуальность конфигурации оборудования и ПО, контактной информации всех лиц, имеющих отношение к данному плану.

В процессе актуализации плана должна быть проведена проверка сроков действия всех договоров на поддержку (гарантийных договоров) систем, включенных в план. Срок действия вышеупомянутых договоров должен быть не менее даты следующего пересмотра настоящего плана (6 месяцев).

Процедура актуализации должна также быть выполнена до планового срока в случае, если в систему вносятся существенные изменения, например, происходит миграция на новое оборудование.

По завершении процедуры актуализации план должен быть заново опубликован и размещен в доступных для ответственных лиц местах.

Частота обновлений компонентов:

- оценка рисков: 6 месяцев;
- стратегия обеспечения непрерывности сервиса:12 мес;
- роли и обязанности команды восстановления:12 мес;
- состав команды восстановления и контактная информация: 3 мес.

Тестирование плана

Тестирование плана аварийного восстановление должно осуществляться на регулярной основе с интервалом не более 6 месяцев. Тестирование плана производится в нерабочее время или в выходные дни.

После получения информации о недоступности сервиса, ответственный администратор, получивший сигнал, должен проинформировать одного из представителей руководства компании о происшествии.

В случае наступления существенного (т.е. такого, который не смог быть оперативно устранен ответственным администратором) сбоя в предоставлении сервиса, служба технической поддержки должна быть незамедлительно проинформирована ответственным администратором.

В случае, если наблюдаются события, которые могут привести к сбою/существенной деградации сервиса в ближайшем будущем, ответственному администратору сначала необходимо провести первичную диагностику, оценить риски и требуемые действия по восстановлению, и потом, в случае существенной вероятности возникновения сбоев в предоставлении сервиса, проинформировать Службу заказчика. В любом случае, сообщение в службу технической поддержки должно содержать следующую информацию:

- сервис(ы), предоставление которых полностью, либо частично, нарушено (может быть нарушено);
- прогнозное время устранения проблемы (если может быть определено на данном этапе);
- возможные альтернативные способы предоставления сервиса, если таковые существуют.

После наступления аварийной ситуации сервисы будут недоступны для пользователей. Службе технической поддержки необходимо проинформировать основных сотрудников, которые используют сервисы.

Мероприятия по обеспечению непрерывности

Фаза 0. Обнаружение инцидента

В течение фазы 0 происходит первичное обнаружение инцидента, возможно лицами, не являющимися специалистами в данном вопросе, первичная оценка степени серьезности повреждений и информирование руководителя АВК.

Любое лицо: если инцидент затрагивает безопасность людей, звонить в спец службы

Группа технической поддержки:

Оценить длительность выхода сервиса из строя (если превышает 1 ч, то информировать АВК)

Администратор сервиса: оценить длительность выхода сервиса из строя

Фаза 1. Идентификация инцидента, выбор стратегии

В течение фазы 1 происходит идентификация характера повреждений специалистами команды АВК, детальная оценка степени серьезности повреждений и производится выбор стратегии восстановления.

Руководитель АВК, специалист, ответственный за поврежденный компонент: проанализировать характер повреждения, оценить время восстановления, принять решение об объявлении аварии или передать инцидент специалисту.

Фазы 2 и 3. Частичное и полное восстановление сервиса

В течение фаз 2 и 3 выполняется процесс частичного и полного восстановления сервиса соответственно. При этом в ходе работ возможно выявления непредвиденных обстоятельств, которые могут привести к изменению уровня инцидента и возврата к этапу выбора стратегии, возможно, с переходом на план более высокого уровня.

Руководитель АВК: определить приоритеты восстановления;

Администратор АВК: проверить достаточность аппаратного обеспечения на момент восстановления.

Ответственный за резервное копирование: проверить достаточность материала резервных копий.

Фаза 4. Выход в штатный режим функционирования

Фаза 4 характеризуется обеспечением полного спектра услуг для бизнес-процессов со стороны ИТ-сервиса, однако, его внутренняя архитектура отличается от штатной (например, отсутствует дублирование компонент).

Руководитель АВК: определить компоненты восстановления системы, получить из резерва недостающие компоненты.

Ответственные лица, администратор сервиса: привести архитектуру сервиса к штатной.

Документирование и анализ инцидента

По окончании процесса восстановления (возможно, до окончания фазы 4) необходимо проведение подробного документирования инцидента и процесса восстановления сервиса от его последствий. Кроме того, анализ процесса восстановления может привести к изменениям в стратегии и планах обеспечения непрерывности сервисов.

Практическая работа 9.
Тестирование планов

После внедрения разработанных документов и соответствующего обучения персонала наступает самый занимательный момент – тестирование разработанных планов и процедур. Как правило, на этом этапе выявляются серьезные недостатки планирования, что в свою очередь ведет к их доработке.

Есть специфические подходы к тестированию, в которых соискателю статуса CISSP необходимо хорошо ориентироваться:

– опрос (checklist test) – проводится методом анкетирования подразделений;

– проход по плану (structured walk-through) – пошаговое «активное» чтение планов всей группой восстановления, выполнение «понарошку» с целью выработки решения об эффективности его положений;

– моделирование (simulation test) – моделирование «виртуального» прерывания каких-либо процессов или сбоя каких-либо компонент системы с целью отработки методов предупреждения и восстановления;

Тестирование осуществляется для проверки работоспособности планов при возникновении определенного набора обстоятельств, влияющих на деятельность компании. План тестирования выбирается с учетом типа компании и ее целей.

Тесты – инструменты оценки, которые используют количественные метрики для проверки работоспособности ИТ-системы или ее компонента.

NIST Special Publication 800-84 «Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities»

К целям тестирования можно отнести:

– получение подтверждений работоспособности планов;

– проверка достаточности методического и технического обеспечения;

– получение необходимых навыков и знаний.

После того как была определена цель тестирования, разрабатывается сценарий, определяется метод тестирования и согласовывается с руководством. Чаще всего применяются следующие методы:

– Настольная проверка (Tabletop);

– Имитация (Imitation);

– Полное тестирование (Full business continuity testing).

После проведения тестирования составляются отчеты, в которых указываются сценарии и результаты тестирования, а также предложения по улучшению планов непрерывности деятельности.

Компании должны выбирать способ тестирования исходя из своих целей и финансовых возможностей. Полное тестирование является самым эффективным так как оно позволяет выявить множество недостатков, но из-за высоких рисков почти не используется на практике. Если компания решила использовать данный вид тестирования, необходимо заручиться поддержкой партнеров или воспользоваться услугами подрядчиков, чтобы минимизировать риски и предупредить значительные простои.

ГЛОССАРИЙ

Анализ воздействия на бизнес (business impact analysis) – Процесс исследования функционирования бизнеса и последствий воздействия на него разрушающих факторов

Анализ эффективности затрат (cost-benefit analysis) – Финансово-экономический метод, применение которого позволяет оценить затраты на МНБ, сопоставить их с полученной от его внедрения выгодой. Выгода может быть определена с позиции финансов, репутации, производства продукции, предоставления услуг, выполнения обязательных требований и т.п.

Бизнес-процесс – совокупность взаимосвязанных мероприятий или работ, нацеленных на создание конкретного товара или услуги для потребителей. Проще говоря, это любая логическая последовательность действий, которая стабильно зациклена и приводит к определенной конечной цели, поставленной перед компанией. Важно уточнить, что коммерческая составляющая не является обязательным элементом в этом вопросе. К примеру, процессы контакта между сотрудниками внутри предприятия (отпуск, перевод, увольнение и т.д.) также могут относиться к бизнес-процессам.

Бизнес-процесс – логическая последовательность человеческих действий (или группы лиц) в рабочем коллективе. Целью его описания является анализ и регламентация определенных событий в штате работников.

Воздействие (impact) – Оцененные последствия для конкретного случая

Возможность реализации (likelihood) – Шансы реализации события, которые определены, измерены и/или оценены объективно или субъективно в терминах общих описаний (маловероятно, вероятно, почти наверняка), частоты или вероятности. Возможность может быть выражена качественно или количественно.

Выгоды (gain) – Положительные последствия

ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования

ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования

ГОСТ Р ИСО 22313-2015 Менеджмент непрерывности бизнеса. Руководство по внедрению

ГОСТ Р 53647.1-2009 Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство

ГОСТ Р 53647.2-2009 Менеджмент непрерывности бизнеса. Часть 2. Требования

ГОСТ Р 53647.3-2015 Менеджмент непрерывности бизнеса. Часть 3. Руководство по обеспечению соответствия требованиям ГОСТ Р ИСО 22301

ГОСТ Р 53647.5-2012 Менеджмент непрерывности бизнеса. Готовность к опасным ситуациям и инцидентам

ГОСТ Р 53647.4-2011/ISO/PAS 22399:2007 Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности

ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса (Переиздание)

ГОСТ Р 53647.6-2012 Менеджмент непрерывности бизнеса. Требования к системе менеджмента персональной информации для обеспечения защиты данных

ГОСТ Р 55235.3-2012 Практические аспекты менеджмента непрерывности бизнеса. Применение к информационным и коммуникационным технологиям

ГОСТ Р 55235.1-2012 Практические аспекты менеджмента непрерывности бизнеса. Менеджмент активов. Требования к оптимальному управлению производственными активами

ГОСТ Р 55235.2-2012 Практические аспекты менеджмента непрерывности бизнеса. Менеджмент активов. Руководство по применению требований к оптимальному управлению производственными активами

ГОСТ Р 53647.8-2013 Менеджмент непрерывности бизнеса. Управление человеческими ресурсами

ГОСТ Р 53647.9-2013 Менеджмент непрерывности бизнеса. Управление организацией в условиях кризиса

Р 50.1.096-2014 Менеджмент непрерывности бизнеса. Руководство по проведению учений и проверке планов непрерывности бизнеса

Р 50.1.095-2014 Менеджмент непрерывности бизнеса. Руководство по организации восстановления после инцидента

Гражданская чрезвычайная (аварийная) ситуация (civil emergency) – Событие или ситуация, представляющие серьезную угрозу для благосостояния людей, окружающей среды в конкретной местности и/или безопасности страны в целом

Деятельность (activity) – Процесс или система процессов, осуществляемых организацией с целью производства одного или более видов продукции, оказания услуг или их поддержки. Примером подобных процессов являются бухгалтерский учет, обеспечение информационных (ИТ) и телекоммуникационных технологий, производство, сбыт.

Допустимый совокупный риск (risk appetite) – величина совокупного риска, который организация готова допустить или которому готова подвергнуться в любой момент времени

Жизненный цикл менеджмента непрерывности бизнеса (business continuity management lifecycle) – совокупность действий по обеспечению непрерывности бизнеса, которые охватывают все аспекты и элементы программы менеджмента непрерывности бизнеса

Инициирование работы (invocation) – объявление о приведении в действие плана обеспечения непрерывности бизнеса организации с целью обеспечения бесперебойности поставки ключевой продукции и/или услуг

Инцидент (incident) – ситуация, которая может произойти и привести к нарушению деятельности организации, разрушениям, потерям, чрезвычайной ситуации или кризису в бизнесе

Контрагент – физическое или юридическое лицо, учреждение или организация, являющееся стороной в гражданско-правовых отношениях, при заключении договора. Контрагентом по отношению друг к другу является каждая из сторон. Каждый из партнеров, подписавших договор, является контрагентом. Контрагенты связаны теми или иными обязательствами согласно подписанному договору

Критические виды деятельности (critical activities) – Виды деятельности организации, которые должны осуществляться для обеспечения поставки ключевой продукции и услуг, позволяющие достигать наиболее важных и первоочередных целей организации

Критические процессы – процессы, ненадлежащая организация которых или несоблюдение требований к их выполнению могут представлять фактическую или потенциальную опасность для обеспечения качества продукции и, следовательно, для эффективности бизнеса

Максимально приемлемый период нарушения (maximum tolerable period of disruption) – Период времени, по истечении которого существует угроза окончательной потери жизнеспособности организации в том случае, если поставка продукции и/или предоставление услуг не будут возобновлены

Менеджмент непрерывности бизнеса МНБ (business continuity management; BCM) – полный процесс управления, предусматривающий идентификацию потенциальных угроз и их воздействие на деятельность организации, который создает основу для повышения устойчивости организации к инцидентам и направлен на реализацию эффективных ответных мер против них, что обеспечивает защиту интересов ключевых причастных сторон, репутации организации, ее бренда и деятельности, добавляющей ценность. Менеджмент непрерывности бизнеса включает в себя управление восстановлением или продолжением деятельности организации в случае нарушений в ее работе, а также общей программой обеспечения непрерывности бизнеса организации путем обучения, практического применения и анализа непрерывности бизнеса, разработкой и актуализацией планов непрерывности бизнеса

Менеджмент риска (risk management) – структурированная разработка и применение культуры, политики, процедур и методов менеджмента к задачам идентификации, анализа, оценки и обработки риска

Нарушение деятельности (организации) (disruption) – невозможность поставки продукции или оказания услуг, установленных в соответствии с целями организации, или перебои в этой деятельности, вызванные ожидаемым (например, забастовка рабочих) или непредвиденным (например, отключение электрической энергии) событием или явлением

Непрерывность бизнеса (business continuity) – стратегическая и тактическая способность организации планировать свою работу в случае инцидентов и нарушения ее деятельности, направленная на обеспечение непрерывности деловых операций на установленном приемлемом уровне

Организация (organization) – группа работников и необходимых средств с распределением ответственности, полномочий и взаимоотношений

Оценка риска (risk assessment) – полный процесс идентификации, анализа и сравнительной оценки риска

План обеспечения непрерывности бизнеса ПНБ (business continuity plan; BCP) – набор документированных процедур и информации, которые разработаны, обобщены и актуализированы с целью их использования в случае возникновения инцидента, и направлены на обеспечение возможности продолжения организацией выполнения критически важных для нее видов деятельности на установленном приемлемом уровне

План управления инцидентом (incident management plan) – точно установленный и документально оформленный план действий, предназначенный для использования при возникновении инцидента, который обычно охватывает вовлеченный персонал, необходимые ресурсы и действия, которые должны быть выполнены в процессе управления инцидентом

Планирование действий в аварийных ситуациях (emergency planning) – разработка и поддержание в рабочем состоянии согласованных процедур организации, направленных на предупреждение, уменьшение масштабов воздействия, смягчение последствий и принятие других мер в случае возникновения аварийных и/или чрезвычайных ситуаций

Последствие (consequence) – результат инцидента, который может повлиять на достижение целей организации. Для каждого инцидента должно быть проведено ранжирование последствий. Последствия могут быть определенными и неопределенными, а также могут иметь позитивное или негативное воздействие на достижение целей организации

Потери (loss) – негативные последствия

Причастная сторона (stakeholder) – любой индивидуум, группа или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными воздействию риска

Программа менеджмента непрерывности бизнеса (business continuity management programme) – процесс постоянного менеджмента, поддерживаемый со стороны высшего руководства и обеспечиваемый необходимыми ресурсами, направленный на осуществление необходимых мер по идентификации воздействия потенциальных потерь, поддержку жизнеспособной стратегии непрерывности бизнеса и планов восстановления бизнеса, а также на обеспечение непрерывности производства продукции и оказания услуг путем обучения и проведения учений, внедрения, анализа и поддержания в рабочем состоянии непрерывности бизнеса организации

Продукция и услуги (products and services) – результат деятельности организации, который она предоставляет своим потребителям, получателям и причастным сторонам, например промышленные товары, страхование, медицинское обслуживание и др.

Риск (risk) – сочетание вероятности события и масштабов его последствий, а также его воздействие на достижение целей организации. Термин «риск» обычно используют только тогда, когда существует возможность негативных

последствий. В некоторых ситуациях риск обусловлен возможностью отклонения от ожидаемого результата.

Стратегия непрерывности бизнеса (business continuity strategy) – способы обеспечения непрерывности бизнеса в организации, направленные на восстановление и продолжение ее деятельности в случае инцидентов, вызывающих нарушение в ее работе

Устойчивость (resilience) – способность организации противостоять воздействию инцидента

Учения (exercise) – мероприятия, в процессе которых частично или полностью проходит отработка действий (репетиция), предусмотренных планом(ами) обеспечения непрерывности бизнеса, направленные на то, чтобы план(ы) содержал(и) необходимую информацию и при выполнении приводил(и) к запланированным результатам. Учения обычно включают в себя инициирование процедуры непрерывности бизнеса, но чаще объявленную или необъявленную имитацию инцидента нарушения непрерывности бизнеса, в процессе которого участники инсценируют возможную ситуацию с целью оценки потенциальных проблем, связанных с их преодолением до наступления реального инцидента.

Целевой срок восстановления (recovery time objective; RTO) – время, запланированное для:

- возобновления производства продукции или оказания услуг после инцидента;
- возобновления деятельности после инцидента;
- восстановления информационной системы и/или прикладных программ после инцидента.

Целевой срок восстановления должен быть меньше, чем максимально приемлемый период нарушения

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Chernova E. V., Gavrilova I. V., Romanova M.V. Dokolin A.S. Information Technology in Business Continuity // Proceedings of the IV International research conference "Information technologies in Science, Management, Social sphere and Medicine" (ITSMSSM 2017). P. 283-286. URL: https://www.atlantis-press.com/proceedings/itsmssm-17/25887889
2. Бизнес-моделирование: IDEF0, DFD, IDEF3, FISHBONE, FTA : учебное пособие / Т.Б. Новикова, О.Б. Назарова. – ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова». – Электрон.текстовые дан. – Магнитогорск: ФГБОУ ВО «МГТУ», 2016.
3. Вихорев С. Эссе о бизнесе, процессах и категорировании КИИ / BIS Journal №3(34). – 2019
4. 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.
5. Гаврилова И.В. Система управления бизнес-процессами Activity BPM / И.В. Гаврилова // Теория и практика применения свободного программного обеспечения. Сборник трудов участников Всероссийской молодежной конференции с элементами научной школы. 2011. С. 147-154.
6. Гончаров А. Выделение бизнес-процессов организации: подход, основанный на результатах процессов // ГК «Современные технологии управления» [сайт]. – URL: https://www.businessstudio.ru/articles/article/vydelenie_biznes_protsessov_organizatsii_podkhod_o/
7. Зуб А. Т. Стратегический менеджмент : учебник и практикум для академического бакалавриата / А. Т. Зуб. – 4-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2019. – 375 с. – (Бакалавр. Академический курс). – ISBN 978-5-534-03013-6. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/432044
8. Инструкции по выполнению практических работ по дисциплине «Управление непрерывностью бизнеса» / Е.В. Чернова – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2021. – 32 с.
9. Информационные технологии в управлении непрерывностью бизнеса / Е.В. Чернова Е.В. [и др.] //Научное обозрение. Экономические науки. 2017. № 5. С. 46-50.
10. Методологии моделирования бизнес-процессов // Центр развития компетенций в бизнес-информатике Высшей школы бизнеса [сайт]. – URL: https://hsbi.hse.ru/articles/metodologii-modelirovaniya-biznes-protsessov-osnovnye-metody-i-metodiki/
11. Мингазов И.М., Чернова Е.В. Исследование критических бизнес-процессов в социальных медиа // Корпоративная экономика. – 2017, № 1 (9). – С. 49-54

12. Мингазов И.М., Чернова Е.В. Обеспечение непрерывности бизнес-процессов в социальных медиа // Перспективы формирования новой экономики XXI века: актуальные достижения региональной науки сборник научных трудов Международной научно-практической конференции. – 2017. – С. 137-142

13. Назарова О.Б. Моделирование бизнес-процессов: учеб.-метод. Пособие / О.Б. Назарова, О.Е. Масленникова. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2015. – 230с.

14. Назарова О.Б., Масленникова О.Е. Теоретические основы моделирования бизнес-процессов: учеб. пособие / О.Б. Назарова, О.Е. Масленникова. – Магнитогорск: Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 159 с.

15. Новикова Т.Б. Aris: теория и практика бизнес-моделирования: учеб. пособие / Т.Б. Новикова, О.Б. Назарова, В.Е. Петеляк. Магнитогорск: Магнитогорск.гос. техн. ун-та им. Г.И. Носова, 2016. – 289 с.

16. Пономаренко К.В., Чернова Е.В. Разработка плана обеспечения непрерывной деятельности компании по предоставлению проектных услуг / Теоретические и прикладные аспекты современной науки : сборник научных трудов по материалам VIII Международной научно-практической конференции 27 февраля 2015 г.: в 7 ч. / Под общ. ред. М.Г. Петровой. – Белгород, ИП Петрова М.Г., 2015. – Часть VII. – 160 с. – с. 123-125 с.

17. Попова Е.В. Угрозы непрерывности бизнеса малого предприятия, занятого высокотехнологичным производством/ Е.В. Попова, Е.В. Чернова // Электронное научно-практическое периодическое издание «Экономика и социум». – 2015. - № 1-1 (14). – С. 599-602

18. Почепский О. Стратегия развития компании: что это такое, как разработать, образцы и примеры // Клеверенс [сайт]. – URL: https://www.cleverence.ru/articles/biznes/strategiya-razvitiya-kompanii-chto-eto-takoe-kak-razrabotat-obrazcy-i-primery/

19. Риб С.И., Кремлева И.В. Различные подходы к выделению и описанию бизнес-процессов // БИТЕК [сайт]. – URL: http://betec.ru/index.php?id=06&sid=50

20. Скокова И.К., Романенко Н.А., Чернова Е.В. Аналитический этап разработки стратегии управления непрерывностью бизнес-процессов для ИТ-компании // Научные труды SWorld. 2016. – Т. 2. № 45. – С. 46-53

21. Совершенствование методов построения причинно-следственных диаграмм для решения задач управления в организационных системах / И.В Гаврилова [и др.] // Фундаментальные исследования. – 2015. № 8-2. – С. 247-251.

22. Чернова Е.В. Профессиональные компетенции магистров бизнес-информатики в курсе «Управление непрерывностью бизнеса» / Научные труды SWorld. – Выпуск 3(44). Том 4. – Иваново: Научный мир, 2016 – 100 с. – с.22-27

23. Чернова Е.В., Чусавитина Г.Н., Чусавитин М.О., Повитухин С.А. Обеспечение непрерывности ИТ-сервисов с использованием программно-определяемых систем хранения данных // Фундаментальные исследования. – 2015. – № 11-3. – С. 524-529

24. Чусавитина, Г.Н., Давлеткиреева, Л.З. Анализ и установление уровня зрелости информационной инфраструктуры организации для управления непрерывностью бизнеса / Л.З. Давлеткиреева, Г.Н. Чусавитина // Современные информационные технологии и ИТ-образование. – 2012. – № 8. – С. 529-544.

Учебное текстовое электронное издание

Чернова Елена Владимировна

УПРАВЛЕНИЕ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

Практикум

Ответственность за содержание возлагается на автора
Издается полностью в авторской редакции

1,90 Мб
1 электрон. опт. диск

г. Магнитогорск, 2022 год
ФГБОУ ВО «МГТУ им. Г.И. Носова»
Адрес: 455000, Россия, Челябинская область, г. Магнитогорск,
пр. Ленина 38

ФГБОУ ВО «Магнитогорский государственный
технический университет им. Г.И. Носова»
Кафедра бизнес-информатики и информационных технологий