Вадим Алджанов

ИТ-АРХИТЕКТУРА ОТ А ДО Я: ШАБЛОНЫ ДОКУМЕНТОВ

Первое издание

Вадим Алджанов

ИТ-архитектура от А до Я: Шаблоны документов. Первое издание

http://www.litres.ru/pages/biblio_book/?art=37395552
ISBN 9785449337634

Аннотация

В книге собраны, обобщены и систематизированы шаблоны и примеры ИТ-документов в таких областях ИТ, как управление ИТ-сервисами, информационной безопасностью и проектами.Книга будут полезна руководителям ИТ-подразделений крупных и средних компаний. Материал изложен в логической последовательности, что дает возможность использования в качестве справочного пособия.

Содержание

ПРЕДИСЛОВИЕ 6
Об авторе 7
Введение 9
Цели книги 12
Сферы, охваченные книгой 13
Благодарность 15
Юридическое уведомление 16
Авторские права 17
Отказ от ответственности 18
ГЛАВЫ КНИГИ 19
УПРАВЛЕНИЕ ИТ СЕРВИСАМИ 20
ОБЩАЯ ИНФОРМАЦИЯ 20
Рекомендации по разработке ИТ документации 23
Методы и техники 24
процессы управления ИТ сервисами 27
Перечень вопросов, регламентирующих ИТ процессы 28
Структура документа «ИТ Стратегия» 32
Структура документа «Устав ИТ» 35
Структура документов «Политики» 36
Структура документа «Архитектура Сервиса» 38

СТРАТЕГИЧЕСКИЕ ДОКУМЕНТЫ ИТ 40
Устав ИТ Департамента 40
Стратегия Информационных Технологий 51
Архитектура Информационных Технологий 57
План Непрерывности Бизнеса 57
План Восстановления после сбоя 73
План Восстановления Бизнеса 86
Стратегический План и бюджет ИТ 89
Конец ознакомительного фрагмента. 92

ИТ-архитектура от А до Я: Шаблоны документов Первое издание

Вадим Алджанов

ISBN 978-5-4493-3763-4
Создано в интеллектуальной издательской системе Ridero

ПРЕДИСЛОВИЕ

Вадим Алджанов

Об авторе

Вадим Алджанов (англ. Vadim Aldzhanov) [Microsoft MCP, MCSA Security, MCSE Security, MCTS, MCITP, MCITP SQL Database Administrator, Cisco CCNA, VMware VCP4, CompTIA A+, Network+, Security+, EC-Council CEH и ECSA, SNIA Certified Storage Professional SCSP, Wireless Technology CWTS, CWNA, CWSP, IT Management ITILv3, Apple Certified Associate – Integration | Management].

В серии книг «ИТ Архитектура от А до Я» собраны и обобщены знания и опыт за более чем 17+ лет работы в ИТ. В течении 14 лет проработал в банковской сфере, большую часть времени на позиции руководителя ИТ департамента. На данный момент являюсь ИТ Архитектором в одном из крупных холдингов страны. Имею степень бакалавра по специальности «Радиотехника» и степень магистра по направлению «Компьютерные Информационные Системы (CIS)». На данный момент продолжаю образование на получение докторской степени по направлению «Менеджмент Информационных Систем (MIS)». Кроме этого имеется порядка тысячи часов обучения на специализированных курсах по направлениям системное администрирование, компьютерные сети, беспроводные сети, системы хранения, системы виртуализации, информационная безопас-

ность, управление ИТ сервисами, управление проектами, банковское дело, пластиковые карты, стратегическое планирование, проведение аудита и прочие. Профиль в LinkedIn: https://www.linkedin.com/in/vadim-aldzhanov-623a7b44/

Введение

Серия книг «ИТ Архитектура от А до Я» является попыткой автора собрать, обобщить и систематизировать накопленный опыт и знания в ИТ области.

Серия книг «ИТ Архитектура от А до Я» – Зеленая книга

Издание «ИТ Архитектура от А до Я: Теоретические основы». Первая книга серии «ИТ Архитектура от А до Я» содержит теоретические основы планирования, построения и сопровождения ИТ архитектуры, управления Проектами, ИТ сервисами и т п. В качестве источника используются как проверенные на практике материалы, так и рекомендации стандартов и практик. Является переработанным, исправленным и дополненным издания «ИТ Архитектура: практическое руководство от А до Я».

Серия книг «ИТ Архитектура от А до Я» – Синяя книга

Издание «ИТ Архитектура от А до Я: Комплексное решение». Вторая книга серии «ИТ Архитектура от А до Я» содержит детальную техническую информацию и практические примеры реализации ИТ решений на основе основ теории, описанной в первой книге. В качестве примеров рассмотрены решения, на базе Windows 10/2016, комплексного решения по мониторингу, управлению и конфигурированию

Microsoft System Center 2016, портал Microsoft SharePoint Server 2016, решения по управлению проектами Microsoft Project Server 2016, почтовый сервер Exchange 2016, решение Skype for Business 2015, функциональные возможности Direct Access 2016, Hyper-V, DFS и File Server, RDS и т п. Представлены детальные требования и примеры расчетов по системам обеспечения. Приведены расчёты мощности и стоимости решений. В качестве примеров используются решения, которые выбраны автором как наиболее подходящие для выполнения поставленных задач, популярные или с которыми автор знаком на практике. Является переработанным, исправленным и дополненным издания «ИТ Архитектура: практическое руководство от А до Я».

Серия книг «ИТ Архитектура от А до Я» – Серая книга

Издание «ИТ Архитектура от А до Я: Шаблоны документов». Сборник содержит набор шаблонов и примеров документации, необходимой в повседневной деятельности ИТ. В качестве источника используются как проверенные на практике материалы, так и рекомендации стандартов и практик.

Серия книг «ИТ Архитектура от А до Я» – Желтая книга

Издание «ИТ Архитектура от А до Я: Каталог решений». Сборник содержит описание возможностей различных ИТ решений, анализ и сравнения функциональных возможно-

стей. На текущий момент протестированы или использованы на опыте более сотни решений.

Серия книг «ИТ Архитектура от А до Я» – Красная книга

Издание «ИТ Архитектура от А до Я: Альтернативное решения». Книга серии «ИТ Архитектура от А до Я» содержит детальную техническую информацию и практические примеры реализации ИТ решений на основе теории, описанной в книге «ИТ Архитектура от А до Я: Теоретические основы». В качестве примеров используются решения, приоритетный критерий выбора которых является «нулевая стоимость». В качестве базового решения принимается ИТ инфраструктура и компоненты, описанные в «Синей книги».

Серия книг «ИТ Архитектура от А до Я» – Черная книга

Издание «ИТ Архитектура от А до Я: Облачное решение». Книга содержит детальную техническую информацию и практические примеры реализации ИТ решений на основе теории, описанной в книге «ИТ Архитектура от А до Я: Теоретические основы». В качестве примеров используются по возможности «облачные» решения.

Цели книги

Книга представляет из себя набор шаблонов и документов необходимых и достаточных для организации деятельности ИТ департамента. В ней содержатся шаблоны и примеры по построению и сопровождению ИТ архитектуры предприятия, организации процессов управления ИТ сервисами и проектами, примеры должностных инструкций, различные формы, акты и типовые отчеты.

Цель книги помочь специалистам и руководителям ИТ разработать необходимый набор ИТ документов. Надлежащее документирование помогает организовать коммуникацию между представителями бизнеса и техническими специалистами, а также сотрудниками организации. Кроме этого позволит подготовить организацию к прохождению ИТ аудита.

Книга не является обязательным руководством по выбору того или иного продукта или решения, а выражает точку зрения автора.

Материал изложен в логической последовательности и снабжен наглядными примерами реализации. Это дает возможность использования данного руководства для методичного изучения аспектов деятельности ИТ, наряду с использованием его в качестве справочного пособия.

Сферы, охваченные книгой

Книга является третьей в серии «ИТ Архитектура от А до Я» и представляет собой руководство на русском языке, в котором собраны шаблоны и примеры документов в области построения Архитектуры Предприятия, Управления Проектами, Информационной Безопасности, Организации и Управления ИТ сервисами и ИТ аудита, позволяющие полностью обеспечить потребности организации в процессе создания и управления ИТ архитектурой и инфраструктурой.

Книга предназначена для широкого круга читателей и будет полезна:

Топ-менеджерам, кураторам ИТ, ИТ директорам крупных и средних компаний так как позволит лучше понимать Архитектуру Предприятия (Enterprise Architecture) на базе подхода (TOGAF), роль и вовлеченность ИТ в бизнес. Показатели распределения финансовых инвестиций на ИТ сервисы. Представители бизнеса смогут понять общие аспекты по функционированию ИТ инфраструктуры, технические термины, принципиальные отличия различных архитектурных решений, принципы построения и сопровождения технических решений. Позволяет сформировать понимаемые обоими сторонами метрики и отчеты по оценке эффективности и результативности функционирования ИТ инфраструктуры.

Руководителям ИТ подразделений, ИТ архитекторам, менеджеров среднего звена ИТ департамента, а также менеджерам проектов книга предоставляет теоретические основы управления ИТ сервисами (ITSM) с применением рекомендаций практик ITIL, интеграцию методики Управление Проектами (PMI) в ИТ, вопросы аудита ИТ (CobiT) и Информационной Безопасности.

Книга не предназначена для малых ИТ инфраструктур т.к. стоимость бумаги выше чем требования, предъявляемые к ИТ. Так же будет мало эффективна для крупных предприятий с корпоративным управлением т.к. по каждому направлению деятельности скорее всего имеются узко направленные эксперты.

Благодарность

Выражаю благодарность друзьям, учителям, руководителям и коллегам за помощь в написании книги, а также бесценный опыт и знания полученный от общения с такими людьми как Александр Буслаев («AIG Group»), Иршад Гулиев («SINAM»), Фазиль Маммедов («ROTABANK»), Яна Хмельницкая и Karsten Stellner («LFS Financial Systems GmbH»), Thomas Engelhardt («Microfinance Bank of Azerbaijan»), Andrew Pospielovsky («ACCESSBANK») и Alan Crompton («Baku European Games Operation Committee BEGOC 2015»).

Юридическое уведомление

Информация, содержащаяся в книге, не несет в себе никакой коммерческой тайны или иной конфиденциальной информации. Материалы собраны из открытых источников, переработаны автором, используя имеющийся опыт и знания. Некоторые рассмотренные примеры приведены только для справки и являются вымышленными. Любое сходство с реально существующими людьми или организациями является случайным. Все упоминающийся в книге названия компаний и продуктов могут быть торговыми марками, принадлежащими соответствующим владельцам.

Авторские права

Отказ от ответственности

Автор не дает никаких гарантий или заявлений о точности, пригодности или полноте информации, ссылок или других предметов, которые содержатся в настоящем документе. Книга доступна всем читателям «как есть» без каких-либо заявлений или гарантий любого рода, явных или подразумеваемых, включая гарантии в отношении товарности или пригодности для определенной цели. Документ может содержать неточности или орфографические ошибки.

Автор не несет никакой ответственности за прямые, косвенные, случайные или прочие убытки при использовании данного руководства. Читатель данного руководства проинформирован.

Посвящается моим родителям, любящей жене и двум прекрасным дочерям.

ГЛАВЫ КНИГИ

Книга включает в себя шаблоны и примеры документов, используемых для построения и сопровождения ИТ Архитектуры Предприятия. Содержание книги:

Раздел I: Управление ИТ Сервисами;

- Глава 1: Стратегические ИТ документы;
- Глава 2: Политики и Положения ИТ;
- Глава 3: ИТ Стандарты;
- Глава 4: ИТ Процедуры;
- Глава 5: Должностные Инструкции;
- Глава 6: Сервисные Соглашения;
- Глава 7: Прочие документы ИТ;

Раздел II: Информационная Безопасность;

- Глава 1: Стратегические документы ИБ;
- Глава 2: Политики и Положения ИБ;
- Глава 3: Стандарты ИБ;
- Глава 4: Процедуры ИБ;
- Глава 5: Должностные Инструкции;
- Глава 6: Прочие документы ИБ;

Раздел III: Управление Проектами;

УПРАВЛЕНИЕ ИТ СЕРВИСАМИ

ОБЩАЯ ИНФОРМАЦИЯ

Перечень необходимых документов сформирован на основе зеленной книги серии. Руководящие документы по управлению ИТ, для удобства, можно разделить по следующим категориям:

•*Политики и положения* – высокоуровневые документы, определяющие общие положения, методы достижения целей, задачи и т п. Определяют высокоуровневые значения (например, … длинна пароля должна быть регламентирована …) Как правило содержит общее описание процедур и принципов.

•*План* – это заранее намеченная система мероприятий, предусматривающая порядок, последовательность и сроки выполнения работ. Как правило хорошо проработанный документ с высоким уровнем детализации.

•*Стандарт* – документы промежуточного уровня, определяющие метрики для методов, определённых в политиках (например, … длина пароля восемь символов…). Наиболее часто изменяемый документ ввиду непрерывности и изменчевости бизнес требований и возможностей организации.

•*Процедуры* – документы промежуточного уровня, опре-

деляющие пошаговый регламент работ для применения политик с использованием метрик стандартов, инструменты, исполнителей, инструкций и т п. как правило глубоко детализированный документ с блок схемами, примерами выполнения действий с конкретной информационной системой. Например, «Процедура Управления Инцидентами» построенная на базе решения Microsoft System Center 2016 Service Manager.

•*Стандартные Операционные Процедуры (СОП)* – документы промежуточного уровня, определяющие пошаговые действия для рутинных работ, указанных в регламенте работ по сервису. К таким работам можно отнести установку сервиса, создание резервной копии, восстановление и т п.

•*Инструкции, акты и формы* – низкоуровневые документы, определяющие действия сотрудников внутри ИТ департамента, конечных пользователей, факты выполнения действий и т п.

В нашем случае, для каждого процесса управления ИТ сервисом, по умолчанию используются три документа: политика, стандарт и процедура. Для идентичных действий, например, порядок разработки, внедрение, утверждение, нумерации и т п, можно использовать отдельный документ по данному под-процессу, и соответственно исключить данную секцию из прочих документов. Для удобства организации работы ИТ и снижения административной нагрузки

можно принять за правило, что, все высокоуровневые и промежуточные документы необходимо подтверждать на ИТ комитете, а низкоуровневые документы могут быть разработаны и утверждены директором ИТ департамента.

Кроме этого, в зависимости от структуры организации некоторые документы могут быть сгруппированы по ролевому принципу. Так для примера, если в организации имеется выделенная роль «Оператора Резервного Копирования», чья задача состоит в создании резервных копий всех ИТ сервисов, то есть смысл сгруппировать процедуры резервного копирования всех ИТ сервисов в одном документе. Это позволит сотруднику поддерживать актуальность информации, и избавит от необходимости просматривания документы «Детальной Архитектуры сервиса» всех сервисов.

Для облегчения создания и работы над такими документами, как детальная архитектура ИТ сервиса, документ может быть разбит на две части:

•*Архитектура сервиса* – описывает назначение, сервиса компоненты, требования, стоимость и т п;

•*Руководство по внедрению и сопровождению* – описывает последовательность развертывания, стандартные операции по сопровождению и т п;

Для небольших организаций, организаций с вялотекущими ИТ процессами, или не значительным влиянием ИТ на бизнес, допускается совмещение политик, процедур

и стандартов различных процессов в едином документе.

Рекомендации по разработке ИТ документации

Ведение документации один из важнейших элементов административной работы и управления. Никто не любит писать документы… кроме тех, кто умеет. Используйте готовые шаблоны и отчетные формы. Но перед тем как начинать придумывать или заполнять готовые шаблоны, нужно ответить на три важных вопроса:

- Какие документы нужны для вашей организации сейчас?
- Насколько детально нужно их прорабатывать?
- Стоимость времени, потраченного на создание документа по отношению к ценности документа?

Генерирование кучу ненужных документов дорого, долго и глупо. Это выгодно, если проект оценивают по толщине отчетных документов. Но толстые документы никто не читает. Их ставят на самую дальнюю полку и забывают навсегда. Поэтому нужно выбрать только те документы, которые нужны, и прорабатывать их настолько детально, насколько это нужно для достижения целей. Логично. Но как определить эту грань? Так как разработка документации и административные работы требуют дополнительных ресурсов, порядок разработки и глубина проработки ИТ документации может

быть различной как для различных организаций, так и отдельных процессов в одной организации. Различают ИТ документы по следующим типам:

По степени важности (Устав, планы, бюджет, политики, стандарты, процедуры, прочие документы).

По уровню взаимодействия:

•Взаимодействие ИТ с внешними организациями;

•Взаимодействие ИТ с подразделениями внутри организации;

•Взаимодействие внутри ИТ департамента;

Методы и техники

Можно руководствоваться различными методами внедрения:

•*«Классический метод»* – разрабатывается документация и процессы собственными силами или с привлечением консультантов и экспертной группы. Внедрение поэтапное основных и второстепенных процессов. В качестве достоинств: наиболее правильный с точки зрения организации. Качественная проработанная цепочка «снизу – вверх» и «сверху-вниз». К недостаткам можно отнести: достаточно затратный как по времени, так и по финансам. Не эффективен в условиях ограниченных ресурсов.

•*«Разработка по требованию»* – процессы формируются в ходе внедрения и сопровождения ИТ сервисов. Да-

лее происходит их обкатка, и лишь затем формальное документирование, и принятие. Приоритеты также формируются по необходимости. Как пример, в первую очередь прорабатываются процессы взаимодействия ИТ и внешних организаций: поставщиками продуктов, компанией разработчиков. Следующий шаг: организуются процессы взаимодействия ИТ департамента с другими подразделениями компании. И в последнюю очередь формализуется организация работ внутри самого ИТ департамента. Достоинства метода: эффективен с точки зрения использования ресурсов, простота и понятность в организации простых процессов, целевой, направлен на управление наиболее важными «живыми» процессами в организации, а не формально «важными» с точки зрения управления ИТ сервисами. Недостатки: часто является реактивным методом, т.е. работает по факту происходящих действий, требует дополнительного времени и ресурсов по интеграции процессов между собой.

•*«Техника постепенного улучшения»* представляет из себя следующую последовательность действий:

- •Выбираете минимальный набор документов;
- •Заполняете документ на основе здравого смысла;
- •Если что-то кажется лишним, отбрасывайте;
- •Оцениваете, сможете ли достичь нужных результатов;
- •Если нет, то включите недостающие разделы;
- •Заполните их и снова проведите оценку;
- •И так далее до достижения результатов.

Выбор метода зависит от индивидуальных особенностей организации и ее культуры. На мой взгляд использование метода «по требованию» с применением техники «постепенного улучшения» является наиболее удачным. Процесс утверждения руководящих ИТ документов в общем случае может выглядеть так:

•Для процессов, владельцем которых является ИТ, или которые являются внутренними процессами ИТ, утверждение возможно по решению ИТ директора с последующим формальным утверждением на ИТ комитете.

•Разрешение конфликта интересов происходит согласно процедуре в два этапа: инициатор и ИТ директор привлекают департамент внутреннего аудита. Если конфликт не разрешен, то запрос эскалируется на ИТ комитет.

•Для процессов, владельцем которых не является ИТ, утверждение возможно только по решению ИТ комитета.

Ряд документов требует разработку их в других департаментах. При этом может соблюдаться следующий алгоритм действий:

•ИТ ссылается на документ, разработанный в соответственном функциональном департаменте (документы по кадрам, закупкам и т п).

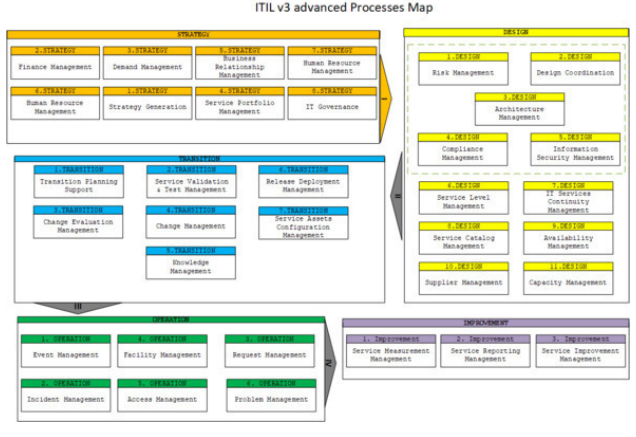
•Если документ отсутствует в функциональном департаменте, то ИТ разрабатывает его самостоятельно по вопросам, связанным с ИТ деятельностью и с учетом вербальных

требований функционального департамента.

•При разрешении конфликтов в различных документах можно руководствоваться принципами наследования «Сверху вниз» и приоритета «Устав – политика – процедура – инструкция».

процессы управления ИТ сервисами

Полноценное управление ИТ сервисами описывается в рекомендациях ITILv3 и CobiT. Основываясь на рекомендациях в книги рассмотрим следующие процессы:



ИТ сервисы

Перечень вопросов, регламентирующих ИТ процессы

Перечень следующих вопросов, регламентирующих ИТ процессы, поможет в их описание в соответствующих руководящих документах:

•*Назначение* – Определение процесса, под-процесса или вид деятельности, и отвечает на вопрос ЧТО (WHAT);

•*Цели* – Определяет цели и задачи процесса, отвечает на вопрос ЗАЧЕМ (WHY) необходима та или иная деятельность;

•*Область применения* – Определяет зону применения данного процесса, отвечает на вопрос КОГДА (WHEN). Определяет триггеры для срабатывания того или иного под-процесса или временные рамки;

•*Зона ответственности* – Определяет зоны ответственности для позиций или группы, отвечает на вопрос КТО (WHO);

•*Процедуры*– Процедуры, связанные с процессом, отвечает на вопрос КАК (HOW). Определяет перечень активности и механизмы для выполнения процесса;

•*Критические Факторы Успеха* (Critical Success Factors CSF) – Определяют, что должно произойти если процесс, сервис или проект будет успешным. Формируются критериями результативности (KGI).

•*Критерии результативности* (KGI) – Определяют критерии результативности достижения целей. Обычно не имеют явно выраженных измеряемых показателей или являются результатом субъективных наблюдений контролирующего органа. Как пример, критерием результативности может являться удовлетворенность бизнеса работой ИТ или процесса. Также может формироваться из показателей KPI.

•*Критерии эффективности* (KPI) – Определяют критерии и метрики эффективности процессов или деятельности, используемых для достижения целей. Как правило формируются из метрик и показателей, которые можно объективно измерить. Как пример, снижение количества инцидентов, ошибок и т п.

•*Карта процесса* – Представляет из себя визуальное описание процесса и деятельности в его рамках.

№	Назначение процесса - (WHAT)	Цели процесса - (WHY)
1	Политики, процедуры по Управлению Требованиями.	Организация процесса Управления Требованиями, обсуждения, внесения изменений и принятие решения.
2	Порядок предоставления требований	Организация процесса предоставления требований
3	Порядок утверждения требований	Организация процесса утверждения требований
4	Контроль и мониторинг состояния	Организация контроля и мониторинга состояния

№	Процедуры – (HOW)	Зона ответственности – (WHO)			
		Responsible R	Authorized A	Involved C	Informed I
1.1	Предоставление требований со стороны бизнеса	дИТ	КИТ		
1.2	Анализ возможности	ИТ	дИТ		
1.3	Обсуждение и принятие решения	ИТ, Бизнес	КИТ		
1.4	Формирование пакета требований и уровня услуг	ИТ, Бизнес	дИТ		
1.5	Утверждение пакета требований и уровня услуг	ИТ, Бизнес	дИТ		
1.6	Контроль за исполнением	ИТ, Бизнес	дИТ		

№	Область применения –(WHEN)	Временные рамки (T)	Пред процесс
1.1	Предоставление требований со стороны бизнеса	Не регламентируется	
1.2	Анализ возможности	+ 14 дней	1.1
1.3	Обсуждение и принятие решения	+ 14 дней	1.2
1.4	Формирование пакета требований и уровня услуг	+ 14 дней	1.3
1.5	Утверждение пакета требований и уровня услуг	+ 14 дней	1.4
1.6	Контроль за соблюдение	непрерывно	1.5

Критерии результативности - (KGI)

KGI Number	KGI Description	KPIs	Collected by	Reported to
DM	Demand Management			
KGI-DM-01	Удовлетворенность бизнеса			

Критерии эффективности - (KPI)

KPI Number	KPI Description	Good	Warning	Collected by	Reported to
DM	Demand Management				
KPI-DM-01	Количество заявленных требований к ИТ				
KPI-DM-02	Количество утвержденных требований	> 70%	<70%		
KPI-DM-03	Количество отклоненных требований по причинам	< 30%			
KPI-DM-04	Количество требований связанных с изменениями				
KPI-DM-05	Количество требований связанных с проектами				
KPI-DM-06	Количество требований выполненных в срок	> 90%	< 90%		
	Полнота соответствия пакета требованиям бизнеса	> 70%	<70%		

Пример описания ИТ процесса

Как видно из примера, критерии результативности могут являться метриками, используемыми при написании политик, а критерии эффективности – метриками и показателями, заявленными в стандарте и используемые при написании процедур.

Стандарт ISO/IEC 20000—1: 2011 рекомендует наличие следующих документов:

- •Procedure for Communication
- •Procedure for Document Control
- •Procedure for Control of Records
- •Procedure for Internal Audit
- •Procedure for Improvements
- •Policy & Procedure for Service Management
- •Procedure for Delivery of New Changes
- •Policy & Procedure for Management Review
- •Procedure for Service Continuity
- •Procedure for Budgeting & Accounting Services
- •Policy & Procedure for Capacity Management
- •Policy & Procedure for Incident Management
- •Procedure to Manage Service Compliance
- •Policy & Procedure for Supplier Management
- •Policy & Procedure for Problem Management
- •Policy & Procedure for Configuration Management
- •Procedure for Organization Security
- •Procedure for Training
- •Policy & Procedure for Availability Management
- •Visitor Policy
- •Policy for Business Relationship Management
- •Change Management Policy
- •Information Security Policy
- •Internet Policy

•Release Management Policy
•Standard Operation Procedures (SOP) for Group Internet & IT Resource Use Procedure
•SOP for E-Mail & Messenger Use
•SOP for Service Continuity Testing
•SOP for Personnel Recruitment
•SOP for Service Reporting
•SOP for Risk Management
•SOP for Business Relationship Management
•SOP for Change Control Management
•SOP for Release & Deployment
•Job Descriptions

Структура документа «ИТ Стратегия»

Структура документа «ИТ Стратегия предприятия». Описание ИТ стратегии целесообразно формировать в виде краткого документа, ориентированного, прежде всего, на бизнес пользователей. Использование технических терминов и аббревиатур должно быть сведено до минимума, насколько это возможно.

Введение

•Цели работы, ограничения и подход – Здесь кратко формулируется назначение документа, определяется его позиционирование для работы ИТ-службы и бизнес-подразделе-

ний, приводятся ссылки на другие документы (описание архитектуры, план проектов).

•Связь со стратегией бизнеса – Здесь описываются внешние и внутренние условия, которые определяют направления развития бизнеса, цели бизнеса и основные инициативы. На основе бизнес-стратегии развития компании формулируются основные задачи информационных систем (что требуется) и ИТ службы (как делать). Определяется позиционирование ИТ для бизнеса организации: например, является ли она конкурентным преимуществом или центром затрат. Здесь можно подчеркнуть роль перспективных информационных технологий для развития существующего бизнеса или создания новых бизнес-направлений.

•Существующая организация дел в области ИТ – Приводится краткое неформальное описание «верхних уровней» архитектуры предприятия. Это могут быть уровни, связанные с бизнес-архитектурой и портфелем прикладных систем или два верхних уровня модели Gartner. Кратко формулируется оценка соответствия существующего состояния архитектуры требованиям бизнеса, основные проблемы ИТ. Может быть приведено резюме по сравнению с конкурентами или с лучшими практиками.

Целевое состояние информационных систем

•Целевая архитектура предприятия (позиционирование/ оценка/ важность) – Для основных направлений бизнеса

приводится резюме по развитию, сохранению или замене соответствующих прикладных систем. Этот раздел не предназначен для описания технических деталей.

•Интеграция – Резюме по организации взаимодействия с внешними системами (поставщики, клиенты), а также приложений между собой, созданию порталов и хранилищ данных и т. п.

•Инфраструктура – При необходимости развития инфраструктуры приводится краткая характеристика направлений развития (модернизация серверов, создание глобальных сетей и т.п.)

Целевая система управления ИТ-ресурсами

•Целевая система управления ИТ ресурсами – Основные направления совершенствования процессов управления ИТ, оценки качества и целевые показатели работы ИТ.

•Организационные изменения – Возможные изменения в структуре управления ИТ, роль CIO. Организация стратегического управления ИТ.

•Взаимодействие – Реализация модели взаимодействия между ИТ- и бизнес подразделениями.

•Сорсинг – Стратегия выбора исполнителей и поставщиков услуг. Развитие персонала внутренней ИТ службы.

•Финансирование – Источники и порядок финансирования, используемые финансовые инструменты, организация принятия решений.

План перехода

•Укрупненный план перехода к целевой архитектуре информационных систем – Интегральные характеристики ИТ-бюджета и списка проектов. Принципы выбора/приоритезации проектов и инструменты для их оценки.

•Варианты и риски – Возможные варианты стратегии в зависимости от объемов финансирования и вариантов развития бизнеса, анализ рисков. Оценка готовности организации к реализации данной стратегии.

•Выбор проектов – Классификация и список важнейших проектов на ближайшие 1—3 года, сгруппированных по категориям. Цель – дать краткое неформальное описание в рамках одного сводного документа (цели, задачи, сроки), а также подчеркнуть вопросы взаимозависимости проектов.

Структура документа «Устав ИТ»

Структура ИТ устава может содержать следующие пункты:

•Общие положения

•Цели документа

•Принятые сокращения и определения

•Сфера действия документа

•Аудитория

•Организация работы с документом

•Цели ИТ департамента
•Задачи ИТ департамента
•Функции ИТ департамента
•Структура ИТ департамента
•Роли и ответственности
•Управление коммуникациями
•Порядок разрешения конфликтов
•Показатели эффективности и критерии оценки деятельности
•Контроль документа
•Контроль версии документа

Структура документов «Политики»

Структура ИТ политики может содержать простую или развернутую структуру. Использование простой структуры имеет смысл, когда она предоставляется на ознакомление всем сотрудникам организации. Ее содержание должно быть максимально простым, понятным и по возможности не объемным. Тем самым сотрудники организации смогут реально ознакомиться с содержанием документа. Простая структура как правило содержит такие пункты как:

•Цели;
•Общие положения;
•Ответственность;
•Описание деятельности;

•Ссылки на документы;

Развернутая структура подходит организации с высоким уровнем зрелости ИТ. Детальность и глубина проработки документа охватывает все аспекты деятельности связанные с сервисом. Также подходит для случаев, когда в наличие имеются только самые необходимые руководящие документы. Отсутствие формального описания таких служебных процессов как управления коммуникацией, разрешения конфликтов, организации работы с документами и т п требует добавления отсутствующих секций в обособленный документ. Развернутая структура может содержать следующие пункты:

•Общие положения
•Цели документа
•Принятые сокращения и определения
•Сфера действия документа
•Аудитория
•Организация работы с документом
•Цели политики (процесса)
•Задачи политики (процесса)
•Процессы и процедуры
Под-процесс 1 (процедура 1)
Под-процесс 2 (процедура 2)
Под-процесс N (процедура N)
•Метрики политики (процесса)

•Роли и ответственности
•Управление коммуникациями
•Порядок разрешения конфликтов
•Влияние при отсутствии документированной политики
•Риски при внедрении и сопровождении политики
•Ключевые факторы успеха внедрения и сопровождения
•Показатели эффективности и критерии оценки деятельности
•Связанные документы, политики или процессы
•Контроль документа
•Контроль версии документа

Структура документа «Архитектура Сервиса»

Детальная Архитектура ИТ сервиса может содержат:
•Название
•Назначение
•Требования
•Ограничения
•Архитектура (физическая и логическая)
•Инфраструктура
•Зависимости и окружения
•Лицензирование
•Мощности
•Масштабирование

- Отказоустойчивость и восстановление
- Резервирование
- Архивирование
- Система обновления
- Роли и ответственности
- Оценка рисков
- Тестирование
- Внедрение
- Установка
- Конфигурирование
- Сопровождение
- Стандартные Операционные Процедуры
- Требования к сотрудникам
- Стоимость
- Индикаторы производительности
- Аудит и контроль логов
- Мониторинг и метрики сервиса
- Управление
- Отчетность
- Рекомендации
- Выводы и уроки
- Дополнения и замечания

СТРАТЕГИЧЕСКИЕ ДОКУМЕНТЫ ИТ

Стратегические документы представляют из себя высокоуровневые документы по руководству деятельностью ИТ департамента в организации. Как правило обсуждение и утверждение данных документов ведется на ИТ комитете и имеет влияние на функционирование всей организации.

Устав ИТ Департамента

ОБЩИЕ ПОЛОЖЕНИЯ

Данный документ регулирует деятельность, организационную структуру, цели и задачи департамента Информационных Технологий (далее используем сокращение ИТ) в организации. Департамент ИТ является структурным подразделением организации и в своей работе руководствуется:

•Действующим законодательством и иными правовыми актами;

•Нормативной документацией Контролирующих органов;

•Уставом организации;

•Уставом ИТ департамента;

•Внутренними документами организации;

•Рекомендациями практик и стандартов, принятых в отрасли;

•Рекомендациями практик и стандартов, принятых в сфере ИТ;

ЦЕЛИ ДОКУМЕНТА

Внесения ясность в процесс организации ИТ департамента, его функционирования, управления, целей, задач и функций.

ПРИНЯТЫЕ СОКРАЩЕНИЕ И ОПРЕДЕЛЕНИЯ

•*Владелец сервиса (service owner)* – роль или структурное подразделение организации, который занимается постановкой целей, принимает решения и управляет финансированием по сервису.

•*Менеджер сервиса (service manager)* – роль или структурное подразделение организации, который занимается выполнением целей и задач, поставленных владельцем сервиса, обеспечивает развертывание и сопровождение сервиса.

•*ИТ* – Информационные Технологии

•*ИБ* — Информационная Безопасность

СФЕРА ДЕЙСТВИЯ ДОКУМЕНТА

Действия данного документа распространяется на все аспекты деятельности организации, относящиеся к компетенции ИТ. Документ является высокоуровневым руководящим документом ИТ департамента и предназначен для ознакомления и соблюдения со стороны руководства структурных

подразделений и сотрудников организации. Документ утверждается решением ИТ комитета и является обязательным для исполнения и соблюдения всеми подразделениями организации. Процедура принятия документа, внесения изменений определены в процедуре «Процедура организации, руководящей ИТ документации».

ЦЕЛИ ИТ ДЕПАРТАМЕНТА

Цели ИТ департаменту со стороны бизнеса ставится ИТ комитетом организации. Основные цели:

•Организация ИТ инфраструктуры организации на уровне, обеспечивающим конкурентное преимущество организации

•Сопровождение ИТ инфраструктуры организации на уровне, необходимом для достижения стратегических и оперативных целей организации

• Обеспечение прозрачности функционирования ИТ департамента

ЗАДАЧИ ИТ ДЕПАРТАМЕНТА

Задачи ИТ департаменту со стороны бизнеса ставится ИТ комитетом организации. Для выполнения целей, поставленных перед ИТ департаментом, на департамент возложен следующий перечень основные задач:

•Организация работы ИТ департамента;

•Разработка Стратегического плана и бюджета ИТ;

•Разработка Оперативных планов и бюджета ИТ;

•Разработка руководящей документации ИТ департамента;

•Соответствие ИТ архитектуры требованиям бизнеса;

•Выбор технологической платформы ИТ инфраструктуры;

•Обеспечение бесперебойного функционирования ИТ инфраструктуры и ее компонентов на требуемом уровне;

•Соблюдение требований Информационной Безопасности;

•Выполнение проектов, связанных с ИТ инфраструктурой;

•Обеспечение мониторинга ИТ инфраструктуры;

•Оптимизация ИТ инфраструктуры и процессов;

ФУНКЦИИ ИТ ДЕПАРТАМЕНТА

ИТ департамент осуществляет свою деятельность на основе стратегических и оперативных планов, утверждаемых руководством организации (ИТ комитетом). В составе организации, ИТ департамент выполняет следующие основные функции:

•Планирование, дизайн, внедрение, сопровождение, улучшение и вывод из эксплуатации компонентов ИТ инфраструктуры;

•Установка, настройка, техническое сопровождение и обслуживание компонентов ИТ инфраструктуры;

•Диагностика и устранение неисправностей компонентов ИТ инфраструктуры;

•Разработка политик, стандартов, процедур и инструкций связанных с функционированием компонентов ИТ инфраструктуры;

•Разработка и сопровождение Планов: Непрерывности Бизнеса, Восстановления после катастроф, Восстановления Бизнеса и т п;

•Подготовка спецификации для закупки компонентов ИТ инфраструктуры;

•Координация работ с поставщиками и разработчиками;

•Координация работ с подрядчиками и субподрядчиками;

•Оказание содействия при проведении аудита;

•Контроль за соблюдением нормативных документов ИТ;

•Предоставление отчетности по функционированию ИТ;

СТРУКТУРА ИТ ДЕПАРТАМЕНТА

Структуру и штатное расписание ИТ департамента утверждается руководителем организации (генеральным директором) по представлению директора ИТ департамента, исходя из целей и задач организации. ИТ департамент является самостоятельным организационной структурой организации. В своей деятельности ИТ департамент подчиняется директору ИТ департамента. Директор ИТ департамента непосредственно подчиняется генеральному директору организации. За постановку целей и задач ИТ департаменту и контроль

за их выполнением отвечает ИТ комитет. В состав ИТ департамента входят функциональные отделы. Руководят отделами менеджеры отделов. Менеджеры отделов непосредственно подчиняются директору ИТ департамента. В состав ИТ департамента входят следующие отделы:

•*Отдел ИНФРАСТРУКТУРЫ* – отдел, отвечающий за функционирование компонентов ИТ инфраструктуры

•*Отдел ПОДДЕРЖКИ ПОЛЬЗОВАТЕЛЕЙ* – отдел, отвечающий за сопровождение компонентов ИТ инфраструктуры на уровне пользователей,

•*Отдел РАЗРАБОТКИ И ПРОГРАММИРОВАНИЯ* – отдел, отвечающий за разработку, внедрение и сопровождение специализированного программного обеспечения, бизнес приложений и их интеграцию.

•*Отдел ИТ БЕЗОПАСНОСТИ* – отдел, отвечающий за функционирование элементов Информационной Безопасности компонентов ИТ инфраструктуры.

В состав отделов входят функциональные подразделения. Руководство подразделением осуществляется руководителем подразделения, непосредственно подчиняющейся менеджеру отдела. В состав ИТ департамента входят следующие подразделения:

•Отдел ИНФРАСТРУКТУРЫ

•Подразделение Системного Администрирования

•Подразделение Сетевого Администрирования

• Подразделение Администрирования Приложений и СУБД

Отдел ПОДДЕРЖКИ ПОЛЬЗОВАТЕЛЕЙ

Отдел РАЗРАБОТКИ И ПРОГРАММИРОВАНИЯ
•Подразделение разработчиков
•Подразделение дизайнеров
•Подразделение бизнес аналитиков
•Подразделение разработчиков СУБД
• Подразделение интеграции

Отдел ИТ БЕЗОПАСНОСТИ
•Подразделение защиты инфраструктуры
• Подразделение защиты приложений

Кроме этого в составе ИТ департамента имеются экспертные позиции, не имеющие штата и подчиняющиеся непосредственно директору ИТ департамента:
•ИТ архитектор
• Менеджер управления проектами

ИТ комитет собирается не реже четырех раз в год. При необходимости, в работе ИТ комитета могут принимать временное участие другие сотрудники организации. Цели, задачи и роли отделов и подразделений детально указаны в по-

ложениях по соответствующим отделам.

РОЛИ И ОТВЕТСТВЕННОСТИ

В соответствии с организационной структурой определены следующие роли:

ИТ КОМИТЕТ – В состав ИТ комитета входит совет директоров (руководители) организации. Кроме этого в состав ИТ комитета входят директора департаментов ИТ и ИБ. Роль ИТ комитета:

•Постановка целей и задач перед ИТ департаментом;

•Утверждение стратегических и оперативных планов ИТ;

•Утверждение стратегических и оперативных бюджетов ИТ;

•Утверждение руководящих документов ИТ департамента;

• Контроль выполнения целей и задач;

Основные принципы в работе ИТ комитета:

•Принятие решения происходит на основе голосования;

•Состав участников голосования должен быть не четный;

•Принятие решения определяется большинством голосов;

•Генеральный директор имеет право блокировать принятие решения;

•Директор ИТ не участвует в голосовании. Он может рекомендовать возможные ИТ решения.

•Директор ИБ не участвует в голосовании.

•Все решения ИТ комитета должны быть документированы.

Директор ИТ – является непосредственным руководителем ИТ департамента. Непосредственно подчиняется генеральному директору организации. Роль и ответственность ИТ директора:

•Постановка задач внутри ИТ департамента;

•Управление ИТ департаментом;

•Предоставление отчетов для ИТ комитета;

•Взаимодействие м другими подразделениями организации;

Экспертная группа – В состав экспертной группы входят профильные специалисты ИТ и бизнеса. Состав группы зависит от обсуждаемого вопроса. Роль и ответственность экспертной группы:

•Обсуждение и анализ технических аспектов требований и задач;

•Формирование технического решения;

Основные принципы в работе экспертной группы:

•Решение группы носит рекомендательный характер;

•Участники голосования имеют равные права;

•При вынесении решения группы на ИТ комитет, реше-

ние должно быть документировано с указанием мнения всех участников;

•Собрания экспертной группы носить нерегулярный характер, и собирается только по необходимости, или как часть проектной команды;

Роли и ответственности сотрудников ИТ департамента указаны в соответствующих должностных инструкциях.

КОММУНИКАЦИЯ

В процессе функционирования ИТ департамента, возникает необходимость взаимодействовать с другими подразделениями организации. ИТ тесно взаимодействует со следующими подразделениями:

•Департамент Информационной Безопасности – по вопросам информационной безопасности. Департамент Информационной Безопасности является владельцем сервисов (services owner), связанных с вопросами безопасности. ИТ департамент является управляющим сервисами (services manager).

•Финансовый департамент – по финансовым вопросам.

•Департамент Управления Кадрами – по вопросам управления персоналом, набор, обучение сотрудников и т п.

•Департамент закупок и снабжения – по вопросам закупки, поставки, гарантированного сопровождения ИТ активов.

•Административный департамент— по вопросам сопро-

вождения систем обеспечения ИТ инфраструктуры.

Все ИТ службы в компаниях, входящих в состав организации функционально подчиняются ИТ департаменту. Порядок взаимодействия, задачи и роли отделов и подразделений детально указаны в соответствующих руководящих документах.

РАЗРЕШЕНИЕ КОНФЛИКТОВ

В процессе функционирования ИТ департамента и взаимодействия с бизнес подразделениями, могут возникать конфликты интересов. Для разрешения конфликтов в организации должен быть разработан и принят процесс разрешения конфликтов. Порядок разрешения конфликтов, если не указан иной, следующий:

•При возникновении конфликта директор ИТ департамента взаимодействует с главой соответствующего департамента. Если конфликт не удалось разрешить, то руководители обращаются к департаменту Внутреннего аудита (горизонтальная эскалация).

•Если и на этом этапе не удалось разрешить конфликт, то он эскалируется на ИТ комитет (вертикальная эскалация).

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ И КРИТЕРИИ ОЦЕНКИ

Критериями оценки деятельности департамента являют-

ся:

•Надежная и безотказная работа всех составляющих ИТ инфраструктуры организации;

•Отсутствие претензий со стороны сотрудников подразделений организации;

•Отсутствие претензий со стороны контролирующих органов по вопросам, относящимся к компетенции ИТ департамента;

•Удовлетворенность руководства организации;

Контроль документа: [•Номер документа: •Наименование документа: •Статус документа: •Маркер безопасности: •Дата утверждения: •Дата вступления в силу: •Протокол ИТ комитета: •Заменяет документ: •Документ разработан: •Дата разработки: •Документ одобрен: •Дата одобрения: •Утвержден: •Дата утверждения:]

Контроль версии документа: [•Версия документа: •Дата внесения изменений: •Автор: • Содержание изменений:]

Стратегия Информационных Технологий

ОБЩИЕ ПОЛОЖЕНИЯ

Данный документ определяет стратегию департамента Информационных Технологий (далее используем сокраще-

ние ИТ) в организации в долгосрочной перспективе.

ЦЕЛИ ДОКУМЕНТА

Внести ясность в концепцию ИТ департамента, формирование ИТ архитектуры. Цели документа:

•Формирование концепции и принципов организации ИТ;

•Своевременное реагирование на изменения бизнеса;

•Повышение эффективности взаимодействия ИТ и бизнеса;

ПРИНЯТЫЕ СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

•*Владелец сервиса (service owner)* – роль или структурное подразделение организации, который занимается постановкой целей, принимает решения и управляет финансированием по сервису.

•*Менеджер сервиса (service manager)* – роль или структурное подразделение организации, который занимается выполнением целей и задач, поставленных владельцем сервиса, обеспечивает развертывание и сопровождение сервиса.

•*Стратегические цели* – определение в общем виде того, какой организация хочет стать в будущем. Относится больше к организации в целом, чем к конкретному подразделению в частности.

•*Стратегические планы* – определяют последовательность действий, этапы по средствам, которых организация

намеревается достигнуть стратегических целей. Обычно ставятся на продолжительный срок, от трех до пяти лет.

•*Тактические планы* – планы по реализации стратегических целей или отдельных его элементов. Обычно ставятся на короткий срок, порядка одного года.

•*Оперативные планы* – планы, обычно поставленные перед конкретными подразделениями организации в установленные сроки, в пределах, установленных в тактических планах. Обычно имеется возможность измерить показатели достижения целей и показатели эффективности.

СФЕРА ДЕЙСТВИЯ ДОКУМЕНТА

Действия данного документа распространяется на все аспекты деятельности организации, относящиеся к компетенции ИТ департамента. Документ является высокоуровневым руководящим документом ИТ департамента и предназначен для ознакомления и соблюдения со стороны руководства структурных подразделений организации и сотрудников. Документ утверждается решением ИТ комитета и является обязательным для исполнения и соблюдения всеми подразделениями организации. Процедура принятия документа, внесения изменений определены в процедуре «Процедура организации, руководящей ИТ документации».

СТРАТЕГИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Стратегия ИТ представляет из себя следующие аспекты:

•ИТ департамент является стратегическим ресурсом организации, призванным обеспечивающим конкурентное преимущество организации, со стороны информационных технологий;

•Централизация функция ИТ департамента по всем компаниям организации;

•Формирование единой ИТ архитектуры организации;

•Формирование единой ИБ архитектуры организации;

•Построение собственного дата центра;

•Консолидация вычислительных ресурсов;

•Централизованное управление, формирование стратегических и оперативных планов и бюджетов, контроль активности ИТ функций;

•Сопровождение ИТ инфраструктуры организации на уровне, необходимом для достижения стратегических и оперативных целей;

• Обеспечение прозрачности деятельности ИТ;

СТРАТЕГИЧЕСКИЕ ЗАДАЧИ ИТ

Задачи ИТ департаменту со стороны бизнеса ставится ИТ комитетом. Основные стратегические задачи:

•Организация работы ИТ департамента;

•Сбор и анализ требований и ограничений бизнеса;

•Разработка Стратегического плана и бюджета ИТ;

•Разработка Оперативных планов и бюджетов ИТ;

•Разработка руководящей ИТ документации;

•Выбор технологической платформы для ИТ инфраструктуры;

•Разработка проекта ИТ Архитектуры Предприятия;

•Построение ИТ Архитектуры Предприятия;

•Сопровождение ИТ на требуемом уровне;

•Обеспечение требуемого уровня Информационной Безопасности;

•Сопровождение бизнес проектов, по вопросам ИТ;

•Оптимизация и модернизация ИТ процессов и инфраструктуры;

РОЛИ И ОТВЕТСТВЕННОСТИ

Определены следующие роли и ответственности:

•ИТ КОМИТЕТ – В состав комитета входит совет директоров организации или направлений бизнеса. Роль и ответственность:

•Постановка стратегических целей и задач перед ИТ;

•Утверждение стратегических целей и задач перед ИТ;

•Контроль выполнения стратегических целей и задач ИТ;

Директор ИТ департамента – является непосредственным руководителем ИТ департамента. Непосредственно подчиняется генеральному директору организации и ИТ комитету. Роль:

•Постановка задач перед ИТ департаментом;

•Управление ИТ департаментом;

•Контроль исполнения поставленных целей и задач;

•Предоставление отчетов;

•Взаимодействие с другими подразделениями организации;

Роли и ответственности сотрудников ИТ департамента указаны в соответствующих должностных инструкциях. Все ИТ службы в компаниях, входящих в состав организации функционально подчиняются ИТ департаменту. Порядок взаимодействия, задачи и роли отделов и подразделений детально указаны в соответствующих руководящих документах.

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ И КРИТЕРИИ ОЦЕНКИ

Критериями оценки деятельности департамента являются:

•Надежная и безотказная работа всех составляющих ИТ;

•Отсутствие претензий со стороны сотрудников организации;

•Отсутствие претензий со стороны контролирующих органов по вопросам, относящимся к компетенции департамента ИТ;

• Удовлетворенность руководства организации;

Контроль документа: [•Номер документа: •Наименова-

ние документа: •Статус документа: •Маркер безопасности: •Дата утверждения: •Дата вступления в силу: •Протокол ИТ комитета: •Заменяет документ: •Документ разработан: •Дата разработки: •Документ одобрен: •Дата одобрения: •Утвержден: •Дата утверждения:]

Контроль версии документа: [•Версия документа: •Дата внесения изменений: •Автор: • Содержание изменений:]

Архитектура Информационных Технологий

Может быть частью ИТ стратегии или отдельным документом. В отличие от ИТ стратегии, которая фокусируется больше на организационных и бизнес вопросах, в ИТ Архитектуре делается упор на техническую и технологическую составляющую. Как правило содержит три основных элемента: архитектура данных, информационных систем и технологий. Цель документа – трансформирование миссии, видения и требований бизнеса в технологическую ИТ архитектуру, набор информационных систем и данные. Полнота и детализация документа зависит от возможности и необходимости.

План Непрерывности Бизнеса

План/Политика Непрерывности Бизнеса (Business

Contingency Plan), определяет порядок реагирования на непредвиденные обстоятельства, ведущие к частичному или полному отказу ИТ сервисов, и их влияние на бизнес. Фокусирует свое внимание на сервисах, отказах и сбоях компонентов инфраструктуры. План определяет шаги, необходимые для восстановления одной или нескольких услуг, события, которые являются основанием для его инициации, людей, которые должны быть задействованы, средства коммуникаций и т. п. Деятельность включает в себя взаимодействие ИТ и бизнеса.

ОБЩИЕ ПОЛОЖЕНИЯ

Данный документ определяет План Непрерывности Бизнеса (Business Contingency Plan BCP) в организации. Документ является стратегическим документом организации. Документ должен соответствовать следующим требованиям:

- Действующему законодательству и иными правовыми актам;
- Нормативной документацией Контролирующего органа;
- Уставу организации;
- Уставу ИТ департамента;
- Внутренним регламентирующими документами;
- Рекомендациям практик и стандартов, принятых в отрасли;
- Рекомендациям практик и стандартов, принятых в ИТ сфере;

ПРИНЯТЫЕ СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

•Владелец сервиса (service owner) – роль или структурное подразделение организации, который занимается постановкой целей, принимает решения и управляет финансированием по сервису.

•Менеджер сервиса (service manager) – роль или структурное подразделение организации, который занимается выполнением целей и задач, поставленных владельцем сервиса, обеспечивает развертывание и сопровождение сервиса.

•Уровень воздействия (impact) – границы воздействия инцидента на функционирование сервиса. Может определяться как степенью отказа сервиса (частичный, полный), так и уровнем охвата пользователей (один сотрудник, группа сотрудников и т п). Является составляющей, определяющей приоритет инцидента.

•Уровень срочности (urgency) – степень, определяющая срочность разрешения инцидента. Является составляющей, определяющей приоритет инцидента.

•Приоритет (priority) – определяет важность инцидента и порядок его разрешения.

•Обходное решение (work around) – действия, позволяющие временно или постоянно устранить инцидент или его причины.

•Эскалация – механизм, позволяющий своевременно устранить инцидент с помощью привлечения дополнитель-

ных ресурсов или компетенции (горизонтальная) или более высокого уровня полномочий (вертикального). Цель данного механизма устранить инцидент в рамках принятого соглашения об обслуживании.

•Анализ Бизнес Процессов (Business Environment Analysis, BEA) – анализ функционирования бизнес процессов и их связь с ИТ;

•Анализ Рисков (Risk Analysis, RA) – экспертная оценка возможных угроз, классификация рисков, вероятность их возникновения, уровень воздействия и механизмы реагирования;

•Оценка Воздействия на Бизнес (Business Impact Analysis, BIA) – анализ Информационной Системы или сервиса на предмет воздействия на бизнес процессы организации;

•Анализ Отказа Сервиса (Service Failure Analysis SFA) – Анализ Информационной Системы или услуги на предмет взаимосвязи с другими системами. Включает в себя анализ воздействия на сервис отказ других систем и воздействие на другие сервисы отказ данного;

•Анализ Отказа Компонентов (Component Failure Impact Analysis CFIA) – анализ сценариев отказа компонентов сервиса;

•Уровень состояния сервиса (Service Delivery Objective SDO) – показатель состояния сервиса на текущий момент. Для каждого сервиса имеется собственный набор атрибутов. В общем случае в качестве таких атрибутов выступает: До-

ступность, целостность и безопасность. Может характеризоваться как «Стандартный», «Приемлемый», «Неудовлетворительный», «Недоступный» и т п;

•Максимально допустимое время сбоя (Maximum Acceptable/Allowable Outage MAO) – Максимально допустимым отключением является время, в течение которого может пройти до того, как неблагоприятное воздействие станет неприемлемым

или невыносимо для предоставления бизнес услуг, продуктов или выполнение бизнес деятельности. Схожие термины: Максимально возможный простой (Maximum Allowable Downtime MAD) или (Maximum Tolerable Downtime MTD).

•Точка Восстановления (Recovery Point Objective RPO) – определяет допустимый уровень потерь;

•Время Восстановления (Recovery Time Objective RTO) – определяет допустимое время на востановление;

•Уровень Восстановления (Recovery Level Objective RLO) – определяет уровень восстановления. Как пример может быть на уровне виртуальной машины, приложения или данных.

ЦЕЛИ ДОКУМЕНТА

Внесения ясность в организацию процесса управления непрерывностью бизнеса. Цели документа:

•Формирование концепции, принципов и организации процесса управления непрерывностью бизнеса в организа-

ции;

•Гарантировать непрерывность бизнеса в установленных рамках;

•Повышение эффективности взаимодействия ИТ и бизнеса;

СФЕРА ДЕЙСТВИЯ ДОКУМЕНТА

Действия данного документа распространяется на все аспекты деятельности организации, затрагиваемых процессом управления непрерывностью бизнеса и ИТ сервисов.

АУДИТОРИЯ

Документ является высокоуровневым руководящим документом и предназначен для ознакомления и соблюдения со стороны всех сотрудников организации.

ОРГАНИЗАЦИЯ РАБОТЫ С ДОКУМЕНТОМ

Документ утверждается решением ИТ комитета и является обязательным для исполнения и соблюдения всеми подразделениями организации. Процедура принятия документа, внесения изменений определены в процедуре «Процедура организации, руководящей ИТ документации».

ЦЕЛИ ПРОЦЕССА УПРАВЛЕНИЯ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

Основные цели политики управления непрерывностью

бизнеса:

•Своевременное реагирование на инциденты и скорейшее восстановление работы бизнеса;

•Формирование процесса управления непрерывностью бизнеса;

•Разработка необходимых процедур, стандартов и метрик;

•Обеспечение прозрачности функционирования ИТ для бизнеса;

•Снижение негативного влияния сбоев на бизнес;

•Рациональное использование ИТ ресурсов;

•Повышения удовлетворенности бизнеса работой ИТ;

•Снижение убытков, связанных со сбоями ИТ;

•Сокращение времени простоя бизнеса;

•Сокращение времени работ по восстановлению бизнеса;

ЗАДАЧИ ПРОЦЕССА УПРАВЛЕНИЯ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

Можно определить следующие задачи по управлению непрерывностью бизнеса:

•Организация процесса управления непрерывностью бизнеса;

•Классификация сбоев;

•Классификация воздействия, срочности и приоритета;

•Классификация метрик и показателей работы процесса;

•Определение ролей и уровня вовлеченности сотрудни-

ков;

•Организации деятельности по своевременному обнаружению;

•Своевременное информирование сотрудников организации;

•Формирование Плана Непрерывности Бизнеса;

•Формирование сценариев сбоев;

•Организации деятельности по устранению сбоев;

•Организация деятельности по восстановлению бизнеса;

•Организации деятельности по расследованию причин сбоя;

•Организации деятельности по коммуникации;

•Организации деятельности по регистрации сбоев;

•Организации взаимодействия с другими ИТ процессами;

•Оптимизация процесса управления непрерывностью бизнеса;

•Организация сценариев тестирования;

ПРОЦЕСС УПРАВЛЕНИЯ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

Основные принципы можно охарактеризовать как:

•Для каждого ИТ сервиса на этапе проектирования должен быть определен механизм непрерывности сервиса;

•Для каждого ИТ сервиса на этапе сопровождения должен быть разработан план обеспечения непрерывности сервиса;

•Для каждого бизнес процесса по возможности должны

быть разработаны «резервный» и «аварийный» планы;

•Процедуры восстановления должны быть прописаны в архитектуре сервиса;

•Метрики должны быть прописаны в архитектуре сервиса;

•Ответственные ИТ сотрудники обязаны незамедлительно реагировать для обеспечения непрерывности сервисов;

•Выборочно, не реже одного раза в год, должно проводиться тестирование плана непрерывности;

Процесс управления непрерывностью бизнеса может включать в себя следующие под-процессы:

•Обнаружение и регистрация

•Классификация и первоначальный анализ

•Расследование и диагностика

•Устранение

•Закрытие

Для построения эффективного процесса управления непрерывностью бизнеса необходимо наличие следующих входных данных:

•Наличие каталога предоставляемых ИТ сервисов;

•Детальная архитектура ИТ сервисов;

•Процедуры по сопровождению ИТ Сервисов;

•Каналы поступления информации;

•Соглашения по уровню предоставлению услуг и метрики;

•Определены группы поддержки;

•Определены каналы обратной связи и коммуникации;
•Наличие компонентной базы ИТ инфраструктуры;

При функционировании процесса управления непрерывностью бизнеса формируются следующие выходных данные:
•Запросы на обслуживание;
•Запросы на изменения;
•Регистрация проблем;
•Записи по инцидентам;
•База знаний;
•Отчеты;
•Сообщения;
•«Резервные» и «Аварийные» планы;
•Инициализация проектов по оптимизации ИТ и бизнеса;

Необходимы следующие инструменты:
•Инструменты для диагностики;
•Инструменты по устранению;
•Инструменты для регистрации;

ИНИЦИАЛИЗАЦИЯ И РЕГИСТРАЦИЯ

Под-процесс обнаружения и регистрации является триггером для запуска процесса. В качестве источников поступления информации о сбое могут выступать:
•Процесс управления событиями;
•Процесс управления инцидентами;

•Автоматизированные средства мониторинга инфраструктуры;

•Информация от сотрудников организации;

•Информация от поставщиков услуг;

•Информация от партнеров;

Последовательность действий включает в себя проверку достоверности информации, регистрацию и информирование владельцев сервиса. Для всех ИТ сервисов, должна быть указана следующая информация:

•Анализ Бизнес Процессов (Business Environment Analysis, BEA);

•Анализ Рисков (Risk Analysis, RA);

•Оценка Воздействия на Бизнес (Business Impact Analysis, BIA);

•Анализ Отказа Сервиса (Service Failure Analysis SFA);

•Анализ Отказа Компонентов (Component Failure Impact Analysis CFIA);

•Оценка влияния на целевую систему;

•Уровень состояния сервиса (SDO);

•Максимально допустимое время сбоя (MAO, MAD или MTD);

•Точка Восстановления (RPO);

•Время Восстановления (RTO);

•Уровень Восстановления (RLO);

•Последовательность действий по восстановлению;

РАССЛЕДОВАНИЕ И ДИАГНОСТИКА

Расследование и диагностика может включать в себя расследование причин сбоя и определение наиболее оптимальных вариантов восстановления.

ОПРЕДИЛЕНИЕ ДЕЙСТВИЙ И МЕХАНИЗМОВ

Механизмы и план действий может быть следующий:

•Если не происходит деградация качества, восстановление выполняется в штатном режиме;

•Если деградация качества в пределах норм, восстановление выполняется в штатном режиме;

•Если деградация качества ниже норм, необходимо проинформировать владельца сервиса. Восстановление сервиса начать в как можно быстрее;

•в случае полного отказа, необходимо проинформировать владельцев текущего и зависимых сервисов. Восстановление начать немедленно. На время восстановления, перейти на «резервный» или «аварийный» план работы бизнеса;

УСТРАНЕНИЕ

В качестве механизмов устранения неисправностей, можно использовать следующие:

•Перезапуск службы или сервиса;

•Перезагрузка сервера;

•Восстановление из резервной копии;

•Переустановка;
•Замена компонентов;

•Восстановление или переустановка может происходить:
•На уровне данных или конфигурации;
•На уровне приложения;
•На уровне операционной системы;
•На уровне виртуальной машины;

После устранения неисправностей необходимо:
•Проверить работоспособность сервиса;
•Проинформировать владельца сервиса;
•Перейти на «штатный» режим работы;
•Обновить информацию;

ЗАКРЫТИЕ

На заключительном этапе проводится анализ сбоя, причины, адекватность плана восстановления и т п. При необходимости инициируются процессы внесения изменений, обновление документации и т.п.

МЕТРИКИ ПРОЦЕССА

Для обеспечения высокого уровня функционирования процесса управления непрерывностью бизнеса необходимо обеспечить мониторинг состояния следующих метрик и активности процесса:

•Количество сбоев;

•Адекватность действий по восстановлению;

•Время восстановления в рамках регламента;

РОЛИ И ОТВЕТСТВЕННОСТИ

В соответствии с организационной структурой организации и ИТ департамента в частности, определены следующие роли:

•Владелец сервиса. Принятие решений (A);

•Менеджер сервиса. Восстановление сервиса в рамках принятого соглашения. Взаимодействие с владельцем сервиса (R);

ВЛИЯНИЕ ПРИ ОТСУТСТВИИ ПРОЦЕССА

Отсутствие процесса управления непрерывностью бизнеса может привести к следующим негативным воздействиям:

•Хаотичный порядок реагирования ИТ при сбоях;

•Хаотичный порядок реагирования сотрудников при сбоях;

•Отсутствие прозрачности по функционированию сервисов;

•Не эффективное использование ИТ ресурсов;

•Финансовые и репутационные потери для бизнеса;

РИСКИ ПРИ ВНЕДРЕНИИ И СОПРОВОЖДЕНИИ ПРОЦЕССА

При внедрении процесса управления ИТ инцидентами в организации могут возникнуть риски, приводящие к неудачному внедрению процесса, или не эффективному его функционированию. Данные риски можно охарактеризовать как:

•Отсутствие поддержки со стороны руководства организации;

•Недостаточный уровень готовности организации и сотрудников;

•Отсутствие необходимых ресурсов, для внедрения процесса;

•Недостатки и ограничения бизнес процессов;

•Нехватка знаний и навыков у специалистов ИТ департамента;

•Недостатки и ограничения информационных системы;

•Недостатки и ограничения сопутствующей ИТ инфраструктуры;

КЛЮЧЕВЫЕ ФАКТОРЫ УСПЕХА ВНЕДРЕНИЯ ПРОЦЕССА

Ключевые факторы успеха при внедрении и сопровождении процесса управления непрерывностью бизнеса:

•Пристальное внимание к процессу;

•Реалистичные цели;

•Оптимальные бизнес процессы;

•Наличие измеряемых метрик и показателей;

•Высокий уровень квалификации сотрудников ИТ;

•Приемлемый уровень осведомленности сотрудников;

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ И КРИТЕРИИ ОЦЕНКИ

Критериями оценки деятельности являются:

•Снижение времени недоступности ИТ для бизнеса;

•Снижение времени восстановления ИТ сервиса;

•Отсутствие претензий со стороны сотрудников;

•Отсутствие претензий со стороны контролирующих органов;

•Удовлетворенность руководства организации;

СВЯЗАННЫЕ ДОКУМЕНТЫ

Действия данного документа дополняется или является основополагающим для следующих ИТ документов:

•Политика, Стандарты и Процедура «Управления Инцидентами»;

•Политика, Стандарты и Процедура «Управления Проблемами»;

•Политика, Стандарты и Процедура «Управления Изменениями»;

•Политика, Стандарты и Процедура «Резервного Копирования»;

•Детальная Архитектура по всем ИТ сервисам;

•Рекомендации стандарта ISO 22301 «Business Continuity»;

Контроль документа: [•Номер документа: •Наименование документа: •Статус документа: •Маркер безопасности: •Дата утверждения: •Дата вступления в силу: •Протокол ИТ комитета: •Заменяет документ: •Документ разработан: •Дата разработки: •Документ одобрен: •Дата одобрения: •Утвержден: •Дата утверждения:]

Контроль версии документа: [•Версия документа: •Дата внесения изменений: •Автор: • Содержание изменений:]

План Восстановления после сбоя

Плана Восстановления после Сбоя (Disaster Recovery Plan). Представляет из себя план восстановления инфраструктуры компании после возникновения аварии, частичной или полной потери ИТ сервиса или его компонентов. Фокусирует свое внимание на воздействиях и их влияние на комплексную ИТ инфраструктуру и бизнес процессы организации. План определяет порядок, сценарии и правила реагирования при возникновении чрезвычайных ситуаций, таких как пожар, наводнение, землетрясение и т п. Как правило, содержит наиболее возможные сценарии чрезвычайных ситуаций и реакцию на них. План должен состоять как минимум из четырех компонентов:

•Сценарии – перечень предполагаемых чрезвычайных си-

туаций.

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

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

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

ОБЩИЕ ПОЛОЖЕНИЯ

Данный документ определяет План Восстановления после Сбоев (Disaster Recovery Plan DRP) в организации. Документ является высокоуровневым, стратегическим руководящим документом. Документ должен соответствовать следующим требованиям:

•Действующему законодательству и иными правовыми актам;

•Требованиям контролирующих органов;

•Уставу организации;

•Уставу ИТ департамента;

•Внутренним регламентирующими документами;

•Рекомендациям практик и стандартов принятых в отрасли;

•Рекомендациям практик и стандартов принятых в ИТ

сфере;

ПРИНЯТЫЕ СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

•Владелец сервиса (service owner) – роль или структурное подразделение организации, который занимается постановкой целей, принимает решения и управляет финансированием по сервису.

•Менеджер сервиса (service manager) – роль или структурное подразделение организации, который занимается выполнением целей и задач, поставленных владельцем сервиса, обеспечивает развертывание и сопровождение сервиса.

•Уровень воздействия (impact) – границы воздействия инцидента на функционирование сервиса. Может определяться как степенью отказа сервиса (частичный, полный), так и уровнем охвата пользователей (один сотрудник, группа сотрудников и т п). Является составляющей, определяющей приоритет инцидента.

•Уровень срочности (urgency) – степень, определяющая срочность разрешения инцидента. Является составляющей, определяющей приоритет инцидента.

•Приоритет (priority) – определяет важность инцидента и порядок его разрешения.

Обходное решение (work around) – действия, позволяющие временно или постоянно устранить инцидент или его причины.

ЦЕЛИ ДОКУМЕНТА

Внесения ясность в организацию процесса управления непрерывностью бизнеса и ИТ сервисов при воздействии внешних факторов. Цели документа:

•Формирование концепции, принципов и организации процесса реагирования на сбой и аварии для обеспечения непрерывности бизнеса в организации;

•Повышение эффективности взаимодействия ИТ и бизнеса;

В документе делается попытка определить наиболее вероятные причины прерывания бизнеса и порядок реагирования в каждом сценарии. План разработан путем анализа того, что прерывается, а не почему. Например, головной офис здания может быть недоступен по многим причинам, но, нас интересует прежде всего, влияния на деятельность организации недоступности здания, а не причины произошедшего (забастовка сотрудников, аварии и т.д.). Очевидно, что организация будет управлять каждым случаем по-разному, в зависимости от причины, но для наших более конкретных целей, здание просто недоступно. План непрерывности бизнеса и аварийного восстановления тесно связан с процедурами и системами резервного копирования.

СФЕРА ДЕЙСТВИЯ ДОКУМЕНТА

Действия данного документа распространяется на все ас-

пекты деятельности организации затрагиваемых процессом управления непрерывностью бизнеса и ИТ сервисов.

АУДИТОРИЯ

Документ является высокоуровневым руководящим документом и предназначен для ознакомления и соблюдения со стороны всех сотрудников организации.

ОРГАНИЗАЦИЯ РАБОТЫ С ДОКУМЕНТОМ

Документ утверждается решением ИТ комитета и является обязательным для исполнения и соблюдения всеми подразделениями организации. Процедура принятия документа, внесения изменений определены в процедуре «Процедура организации, руководящей ИТ документации».

ЦЕЛИ ПРОЦЕССА

Основные цели можно определить, как:

- Своевременное реагирование;
- Скорейшее восстановление;
- Формирование процесса реагирования на катастрофы;
- Определение процедур, стандартов и метрик;
- Обеспечение прозрачности функционирования ИТ;
- Снижение негативного влияния сбоев на бизнес;
- Рациональное использование ИТ ресурсов
- Повышения удовлетворенности бизнеса и сотрудников;
- Снижение убытков, связанных со сбоями;

•Сокращение времени простоя бизнеса;
•Сокращение времени восстановления бизнеса;

ЗАДАЧИ ПРОЦЕССА

Можно определить следующие задачи :

•Организация процесса;
•Классификация воздействий и сбоев;
•Определение метрик и показателей;
•Определение обязанностей и уровня вовлеченности сотрудников;
•Организации деятельности по своевременному обнаружению;
•Формирование Плана Восстановления после сбоя;
•Формирование сценариев чрезвычайных ситуаций;
•Организации деятельности по устранению сбоев;
•Организации деятельности по устранению последствий;
•Организация деятельности по восстановлению бизнеса;
•Организации деятельности по расследованию причин сбоя;
•Организации деятельности по коммуникации;
•Организации деятельности по реагированию;
•Организации взаимодействия с другими процессами;
•Оптимизация процесса восстановления после сбоя;
•Организация сценариев тестирования;

ПРОЦЕСС ВОССТАНОВЛЕНИЯ ПОСЛЕ СБОЕВ

План восстановления после сбоя представляет из себя различные сценарии, которые могут привести к значительным негативным воздействиям на бизнес. Сценарии описываются набором метрик и значений, представленных в таблице.

Таблица I: определения возможных рисков / (Сценарий, риска)

ОПИСАНИЕ РИСКОВ	Описание
Вероятность события	вероятность риска возникновения (высокая, средняя, низкая)
Вероятный сценарий	наиболее вероятной причины проблемы происходят
Влияние	влияние на наш бизнес будет высокий, средний или низкий
Затронутые функции	какие функции, связанные с документом проблемы воздействия
Оценка рисков	сочетание вероятности и влияния дать общей мерой риска
Место сборка	замещение здания, объект или помещение
Смягчение последствий	что делается для сведения к минимуму риска, прежде чем это произойдет
Команды восстановления	Группы сотрудников, ответственные за конкретные действия и задачи в случае наступления события данного риска
Цели восстановления	Ключевые цели
Функции и обязанности групп восстановления: кто и чем занимается, штатное расписание, и т.д.	

Атрибуты и метрики сценариев

Основные принципы можно охарактеризовать как:

•Для каждого ИТ сервиса на этапе проектирования должен быть определен механизм непрерывности сервиса;

•Для каждого ИТ сервиса на этапе сопровождения должен быть разработан план обеспечения непрерывности сервиса;

•Для каждого бизнес процесса должны быть разработаны «резервный» и «аварийный» планы;

•Процедуры восстановления и метрики должны быть описаны;

•Ответственные сотрудники обязаны незамедлительно реагировать для обеспечения непрерывности или восстановления;

•Должно проводиться тестирование плана;

СЦЕНАРИЙ №1 «Воздействие стихийных бедствий»

•Описание Риска: Потеря здания головного офиса;

•Вероятность события: Низкая;

•Вероятный причины: Пожар, землетрясение, наводнение и т п;

•Влияние: Очень высокое;

•Затронутые функции: Вся деятельность бизнеса;

•Оценка рисков: Высокая;

•Место сбора: Сотрудники головной офис собираются в филиале «Филиал №1»;

•Смягчение последствий: Предопределенные и испытанные политики, процедуры и план действий на местах;

•Команда восстановления: Комитет по реагированию на Чрезвычайные Ситуации (Кризисный Комитет), Группы реагирования от каждой бизнес функции, ИТ, Безопасности;

Цели команд восстановления:

•Этап восстановления №1 т.е. восстановить минимальный уровень обслуживания в течении 24 часов;

•Этап восстановления №2 – восстановление полного уровня обслуживание всех бизнес функций в течении 72 ча-

сов;

Функции и обязанности групп восстановления:

•Кризисный Комитет – Принятие решения по переходу на резервный план, выполнение плана восстановления, и принятие решений по дальнейшему управлению, в полоть до полного восстановления;

Группы реагирования от каждой бизнес функции – выполнение работ по переходу на резервный план и восстановлению операций.

План действий: <детальное описание>

Заключение и рекомендации: <детальное описание>

ПРОЦЕСС ТЕСТИРОВАНИЯ

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. Цели тестирования:

•Получение подтверждений работоспособности планов;

•Проверка достаточности методического и технического обеспечения;

•Получение необходимых навыков и знаний;

После того как была определена цель тестирования, раз-

рабатывается 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.

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:

- Изменение ИТ инфраструктуры;
- Изменение организационной структуры компании;
- Изменения в законодательстве;
- 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 теоретические и практические тренинги для сотрудников организации, по выполнению плана;

•Интегрировать вопросы непрерывности бизнеса в процесс управления изменениями компании;

МЕТРИКИ ПРОЦЕССА

Для обеспечения высокого уровня функционирования процесса управления непрерывностью бизнеса необходимо обеспечить мониторинг состояния следующих метрик и активности процесса:

•Адекватность действий по восстановлению;

•Время восстановления в рамках регламента;

РОЛИ И ОТВЕТСТВЕННОСТИ

В соответствии с организационной структурой организации и ИТ департамента в частности, определены следующие роли и ответственности:

ВЛИЯНИЕ ПРИ ОТСУТСТВИИ ПЛАНА

Отсутствие процесса восстановления после сбоя может привести к следующим негативным воздействиям:

•Хаотичный порядок реагирования ИТ;

•Хаотичный порядок реагирования сотрудников;

•Отсутствие прозрачности функционирования ИТ и бизнеса;

•Не эффективное использование ИТ ресурсов;

•Финансовые и репутационные потери для бизнеса;

РИСКИ ПРИ ВНЕДРЕНИИ И СОПРОВОЖДЕНИИ

При внедрении в организации могут возникнуть риски, приводящие к неудачному внедрению процесса, или не эффективному его функционированию. Данные риски можно охарактеризовать как:

•Отсутствие поддержки со стороны руководства организации;

•Недостаточный уровень готовности организации и сотрудников;

•Отсутствие необходимых ресурсов, для внедрения процесса;

•Недостатки и ограничения бизнес процессов;

•Нехватка знаний и навыков у специалистов ИТ департамента;

•Недостатки и ограничения информационных системы;

•Недостатки и ограничения сопутствующей ИТ инфраструктуры;

КЛЮЧЕВЫЕ ФАКТОРЫ УСПЕХА ВНЕДРЕНИЯ ПРОЦЕССА

Ключевые факторы успеха:

•Пристальное внимание к процессу;

•Реалистичные цели;

•Оптимальные бизнес процессы;

•Наличие измеряемых метрик и показателей;

•Высокий уровень квалификации сотрудников ИТ;

•Приемлемый уровень осведомленности сотрудников;

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ И КРИТЕРИИ ОЦЕНКИ

Критериями оценки деятельности являются:

•Снижение времени недоступности ИТ для бизнеса;

•Снижение времени восстановления ИТ сервиса;

•Отсутствие претензий со стороны сотрудников;

•Отсутствие претензий со стороны контролирующих органов;

•Удовлетворенность руководства организации;

СВЯЗАННЫЕ ДОКУМЕНТЫ

Действия данного документа дополняется или является основополагающим для следующих ИТ документов:

•Политика, Стандарты и Процедура «Управления Инцидентами»;

•Политика, Стандарты и Процедура «Управления Проблемами»;

•Политика, Стандарты и Процедура «Управления Изме-

нениями»;

•Политика, Стандарты и Процедура «Резервного Копирования»;

•Детальная Архитектура по всем ИТ сервисам;

•Политика и план «Управления Непрерывностью Бизнеса»;

•Рекомендации стандарта ISO 22301 «Business Continuity»;

•Рекомендации стандарта ISO 20000 «IT Service Management»;

•Рекомендации стандартов ISO 27000 «Information Security»;

Контроль документа: [•Номер документа: •Наименование документа: •Статус документа: •Маркер безопасности: •Дата утверждения: •Дата вступления в силу: •Протокол ИТ комитета: •Заменяет документ: •Документ разработан: •Дата разработки: •Документ одобрен: •Дата одобрения: •Утвержден: •Дата утверждения:]

Контроль версии документа: [•Версия документа: •Дата внесения изменений: •Автор: • Содержание изменений:]

План Восстановления Бизнеса

Плана Восстановления Бизнеса (Business Continuity Plan)

имеет схожее значение, что и План Непрерывности Бизнеса (Business Contingency Plan), но фокусируется на восстановлении предоставления ИТ сервисов вне зависимости от степени воздействия. Определяет восстановление бизнеса после значительного ущерба в следствии воздействия катастроф. Фактически, данный план является продолжением деятельности «Плана непрерывности Бизнеса» + «Плана Восстановления после сбоя». Но, в отличие от них, может включать в себя стратегические изменения в каталоге ИТ сервисов после воздействия чрезвычайной ситуации. Документ может быть разбит на два плана управления непрерывностью:

•План восстановления ИТ услуг (IT Service Continuity Plan) – план, определяющий шаги, необходимые для восстановления одной или нескольких услуг. План также должен определять события, которые являются основанием для его инициации, людей, которые должны быть задействованы, средства коммуникаций и т. п.

•План восстановления бизнеса (Business Continuity Plan BCP) – план определяет шаги, необходимые для восстановления бизнес-процессов в случае нарушения их функционирования. План также должен содержать информацию о событиях, которые являются основанием для его инициирования, людях, которые должны быть задействованы в реализации плана, средствах коммуникаций и т. п.

Примерная структура плана восстановления 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;

Помимо основных элементов, таких как проведение BIA, определения превентивных мер, стратегии восстановление, плана реагирования на воздействия, структура документа дополнительно должна регламентировать следующую деятельность:

- Формирование команды по оценки ущерба;
- Оценку ущерба;
- Формирование команды по восстановление;
- Выполнение плана восстановления;

Для формирования и выполнения плана может понадобится наличие следующих команд:

•Команда по восстановлению (Restoration Team)

•Команда по оценке ущерба (Damage Assessment Team)

•Команда по спасению активов (Salvage Team)

Стратегический План и бюджет ИТ

ОБЩИЕ ПОЛОЖЕНИЯ

Данный документ определяет цели и задачи департамента Информационных Технологий (далее используем сокращение ИТ) в организации в долгосрочной перспективе. Как правило подразумевается трех летний или пяти летний срок.

ЦЕЛИ ДОКУМЕНТА

Внесения ясность в постановку долгосрочных планов ИТ департаменту, его функционирования, управления, целей, задач и функций. Цели стратегического планирования:

•Формирование долгосрочных целей и задач для ИТ департамента, для достижения долгосрочных целей и задач организации.

•Своевременное реагирование на изменения или отклонения между фактическими и утвержденными планами

•Повышение эффективности взаимодействия ИТ департамента и бизнеса.

ПРИНЯТЫЕ СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

•*Владелец сервиса (service owner)* – роль или структурное подразделение организации, который занимается постановкой целей, принимает решения и управляет финансированием по сервису.

•*Менеджер сервиса (service manager)* – роль или структурное подразделение организации, который занимается выполнением целей и задач, поставленных владельцем сервиса, обеспечивает развертывание и сопровождение сервиса.

•*Стратегические цели* – определение в общем виде того, какой организация хочет стать в будущем. Относится больше к организации в целом, чем к конкретному подразделению в частности.

•*Стратегические планы* – определяют последовательность действий, этапы по средствам, которых организация намеревается достигнуть стратегических целей. Обычно ставятся на продолжительный срок, от трех до пяти лет.

•*Тактические планы* – планы по реализации стратегических целей или отдельных его элементов. Обычно ставятся на короткий срок, порядка одного года.

•*Оперативные планы* – планы, обычно поставленные перед конкретными подразделениями организации в установленные сроки, в пределах, установленных в тактических планах. Обычно имеется возможность измерить показатели достижения целей и показатели эффективности.

СФЕРА ДЕЙСТВИЯ ДОКУМЕНТА

Действия данного документа распространяется на все аспекты деятельности организации, относящиеся к компетенции ИТ департамента. Документ является высокоуровневым руководящим документом ИТ департамента и предназначен для ознакомления и соблюдения со стороны руководства структурных подразделений организации и сотрудников. Документ утверждается решением ИТ комитета и является обязательным для исполнения и соблюдения всеми подразделениями организации. Процедура принятия документа, внесения изменений определены в процедуре «Процедура организации, руководящей ИТ документации».

СТРАТЕГИЧЕСКИЕ ЦЕЛИ

Цели ИТ департаменту со стороны бизнеса ставится ИТ комитетом организации. Формирование Плана Стратегического развития ИТ департамента основывается на Плане Стратегического развития организации. Основные стратегические цели ИТ департамента:

•Организация ИТ инфраструктуры организации на уровне, обеспечивающим конкурентное преимущество организации

Конец ознакомительного фрагмента.