



**РАЗРАБОТКА МЕТОДИК И РЕГЛАМЕНТОВ
В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Неправильно построенная система управления ИТ приводит к следующим последствиям:

- ▶ Сложность управления и контроля ИТ.
- ▶ Неопределенность в текущем и целевом состоянии ИТ.
- ▶ Отсутствие детализированных ИТ-целей, отсутствие привязки ИТ-целей к ИТ-процессам.
- ▶ Отсутствие возможности измерения работы ИТ-процессов, отсутствие управленческой отчетности по ИТ.
- ▶ Отсутствие привязки ИТ-проектов к ИТ-целям.



Международные стандарты и лучшие практики адаптируются и используются с учетом отраслевой специфики деятельности Заказчика и в соответствии с требованиями российского законодательства.



Внедрение передовых методик в области управления ИТ, документирование и контроль ИТ-деятельности позволяет достигнуть следующих важных результатов:

- ▶ Повышение эффективности и управляемости ИТ.
 - ▶ Повышение управляемости и прозрачности работы ИТ-службы.
 - ▶ Оперативность реагирования ИТ на требования бизнеса.
 - ▶ Возможность измерения результатов ИТ-деятельности.
 - ▶ Четкое понимание текущего и целевого состояния ИТ.
 - ▶ Направленность оперативных действий ИТ-подразделений на достижение стратегических ИТ-целей.
- Компания ОТР предоставляет услуги по разработке методик, высокоуровневых политик и детальных регламентов/процедур в области информационных технологий и информационной безопасности.
- ▶ Повышение мотивации ИТ-специалистов.

1. Управление ИТ

- ▶ Разработка нормативно-методических документов по управлению ИТ.
- ▶ Разработка детальных регламентов в области управления и контроллинга ИТ.
- ▶ Разработка положений и должностных инструкций по ИТ-процессам.

2. Внутренний контроль ИТ

- ▶ Разработка методики внутреннего контроля ИТ.
- ▶ Разработка методики внутреннего аудита ИТ.
- ▶ Разработка методики внутреннего аудита информационной безопасности.

3. Управление ИТ-рисками

- ▶ Разработка положения по управлению ИТ-рисками.
- ▶ Разработка процедур по управлению ИТ-рисками.

4. Служба поддержки пользователей (Service Desk)

- ▶ Разработка положения о службе Service Desk.
- ▶ Разработка регламентов и процедур по предоставлению ИТ-сервисов.

5. Обеспечение информационной безопасности

- ▶ Разработка политики в области обеспечения информационной безопасности.
- ▶ Разработка регламентов и процедур обеспечения информационной безопасности.

Система управления ИТ должна строиться на основе системного подхода и в соответствии со стандартами и лучшими практиками.

В рамках услуги могут быть выполнены следующие работы.

Разработка концепций и политик

- ▶ Концептуальная модель/система управления ИТ.
- ▶ Лицензионная политика в области ИТ.
- ▶ Политика в области ИТ-аутсорсинга.

Разработка (внедрение/сопровождение) методик

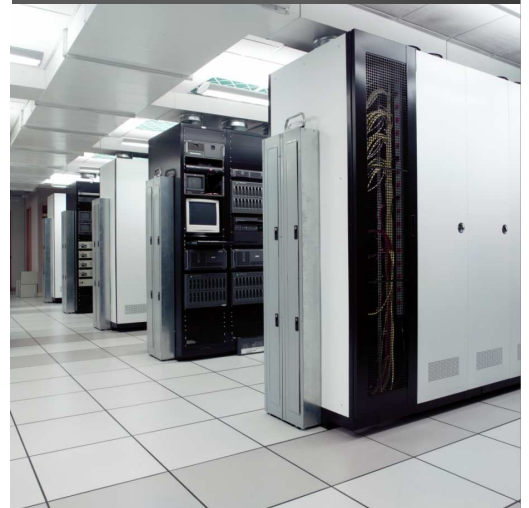
- ▶ Методика управления ИТ.
- ▶ Методика контроллинга ИТ-деятельности (критерии и метрики оценки, шаблоны управленческой отчетности).
- ▶ Методика управления ИТ-проектами.
- ▶ Методика ИТ-бюджетирования.

Разработка (сопровождение) регламентов

- ▶ Регламенты по ИТ-процессам (общая процессная модель ИТ-процессов, положения по отдельным ИТ-процессам, детальные модели ИТ-процессов, модели зрелости ИТ-процессов, матрица владельцев ИТ-процессов).
- ▶ Регламенты ИТ-службы (организационная модель, положения о подразделениях, должностные инструкции).
- ▶ Положение о резервном копировании и восстановлении данных.
- ▶ Положение об управлении ИТ-инфраструктурой.
- ▶ Порядок управления ИТ-проектами.
- ▶ Порядок тестирования и установки обновлений программного обеспечения.
- ▶ Порядок хранения дистрибутивного программного обеспечения и документации.
- ▶ Порядок документирования программного обеспечения.
- ▶ Порядок проведения тендеров.
- ▶ Порядок обучения пользователей.
- ▶ Порядок пересмотра ИТ-бюджета.

В качестве расширения услуги дополнительно могут быть выполнены следующие работы:

- ▶ Сбор и формализация требований к информационной системе управления и контроля ИТ-процессов.
- ▶ Постановка задач на разработку/доработку информационной системы управления и контроля ИТ-процессов.
- ▶ Обзор рынка и анализ соответствия информационных систем управления и контроля ИТ-процессов.
- ▶ Доработка/настройка выбранной информационной системы управления и контроля ИТ-процессов.
- ▶ Внедрение информационной системы управления и контроля ИТ-процессов на пилотном участке.
- ▶ Тиражирование системы в филиалы Заказчика.



Используемые лучшие практики и стандарты:

- ▶ COBIT.
- ▶ ITIL/ITSM.
- ▶ ISO/IEC 20000.
- ▶ ISO/IEC 15504 (SPICE).
- ▶ PMBoK/PRINCE2.
- ▶ CMMI.

Внутренний контроль ИТ

Компоненты внутреннего контроля:

- ▶ Контрольная среда.
- ▶ Оценка риска.
- ▶ Контрольные процедуры.
- ▶ Информация и коммуникации.
- ▶ Мониторинг.

В качестве расширения услуги дополнительно могут быть выполнены следующие работы:

- ▶ Внедрение системы внутреннего контроля ИТ, системы внутреннего аудита ИТ.
- ▶ Сбор и формализация требований к ИС внутреннего контроля ИТ.
- ▶ Обзор рынка и анализ соответствия ИС внутреннего контроля ИТ.
- ▶ Доработка/настройка выбранной ИС внутреннего контроля ИТ.
- ▶ Внедрение и тиражирование ИС внутреннего контроля ИТ.



Используемые лучшие практики:

- ▶ 242-П (Положение ЦБ РФ).
- ▶ COBIT.
- ▶ COSO.
- ▶ SOX 404.

Внутренний контроль – процесс, осуществляемый Советом директоров, менеджментом и другим персоналом организации, направленный на обеспечение разумной гарантии достижения следующих целей: эффективности деятельности, достоверности финансовой отчетности, соблюдения соответствующих законодательных и нормативных актов (COSO Framework, 1992).

В рамках разработки/адаптации методики внутреннего контроля ИТ выполняются следующие работы:

- ▶ Аудит критичных для бизнеса ИТ-ресурсов на готовность к реагированию на возникающие угрозы.
- ▶ Выделение неуправляемых ИТ-рисков и ИТ-процессов (или их элементов), не создающих стоимости для бизнеса.
- ▶ Детализация системы индикаторов ИТ-рисков.
- ▶ Идентификация объектов контроля в разрезе ИТ-процессов.

Внутренний аудит – деятельность по предоставлению независимых и объективных гарантий и консультированию, направленная на совершенствование деятельности организации.

В рамках разработки/адаптации методики внутреннего аудита ИТ выполняются следующие работы:

- ▶ Проведение обследования (оценка зрелости ИТ-процессов управления ИТ и соотнесение с эталонной моделью, анализ рисков в области управления ИТ).
- ▶ Концептуальное проектирование (определение целей и задач, информационного обеспечения, ресурсов, критериев аудита, принципов оценки, методов сбора информации, принципов планирования аудита, ролей и ответственности, показателей эффективности).
- ▶ Определение показателей и метрик ИТ-процессов.
- ▶ Определение процедур оценки.
- ▶ Детальное описание процедур оценки.
- ▶ Разработка документации (рабочие инструкции, запросы, распоряжения, отчеты, анкеты).
- ▶ Разработка программы обучения.
- ▶ Разработка программы и планов аудита.

В качестве расширения услуги может быть разработана/адаптирована методика внутреннего аудита ИБ. При этом дополнительно выполняются следующие специфичные виды работ:

- ▶ Анализ политики ИБ.
- ▶ Анализ физической реализации логической структуры информационных потоков.
- ▶ Детальное изучение каждого в отдельности критического компонента ИС.
- ▶ Проведение работ по обнаружению уязвимостей, специфичных для каждого компонента ИС.

Управление рисками – процесс, осуществляемый Советом директоров, менеджментом и другими сотрудниками, который начинается при разработке стратегии и затрагивает всю деятельность организации и направленный на определение событий, которые могут влиять на организацию, и управление связанными с этими событиями риском, а также контроль того, чтобы не был превышен риск-аппетит организации и предоставлялась разумная гарантия достижения следующих целей: стратегические и тактические цели, эффективность деятельности и сохранность ресурсов, достоверность отчетности (не только финансовой), соблюдение соответствующих законодательных и нормативных актов (COSO ERM, 2004).

Жизненный цикл системы управления ИТ-рисками:

- ▶ Идентификация и анализ ИТ-рисков.
- ▶ Качественная и количественная оценка ИТ-рисков.
- ▶ Принятие ИТ-рисков.
- ▶ Мониторинг и контроль ИТ-рисков.

При разработке/адаптации методики управления ИТ-рисками выполняются следующие работы:

- ▶ Выделение наиболее затратных и угрожающих стабильности бизнеса областей.
- ▶ Ранжирование ИТ-рисков в этих областях по критичности, возможному урону и вероятности наступления.
- ▶ Построение сценариев развития событий и оценка их критичности для компании.
- ▶ Определение индикаторов ИТ-рисков, способов нивелирования и реагирования на ИТ-риски.
- ▶ Выявление, расстановка в приоритетном порядке и разработка мероприятий по упреждению ИТ-рисков.
- ▶ Разработка карты ИТ-рисков.
- ▶ Подготовка плана действий по снижению ИТ-рисков.

В рамках услуги могут быть разработаны следующие документы:

- ▶ Политика управления ИТ-рисками
- ▶ Политика управления рисками ИБ.

Достижимые результаты:

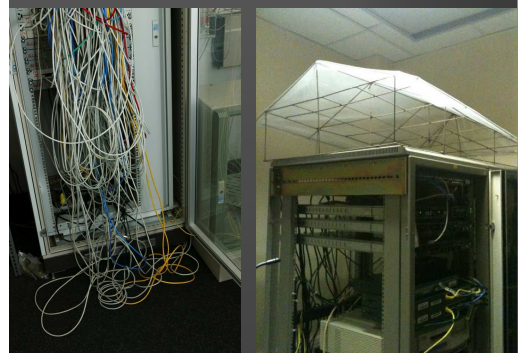
- ▶ Минимизация рисков бизнеса, связанных с ИТ.
- ▶ Повышение прозрачности бизнеса.
- ▶ Повышение уверенности в достижении целей и сохранности активов.
- ▶ Повышение эффективности принятия управленческих решений.

В рамках разработки/адаптации методики управления ИТ-рисками рассматриваются риски в области управления ИТ-процессами, управления ИС, управления ИТ-проектами, управления ИТ-инфраструктурой.

Компоненты управления рисками:

- ▶ Внутренняя среда.
- ▶ Постановка целей.
- ▶ Определение событий.
- ▶ Оценка рисков.
- ▶ Реагирование на риск.
- ▶ Средства контроля.
- ▶ Информация и комментарии.
- ▶ Мониторинг.

В качестве расширения услуги осуществляется внедрение системы управления ИТ-рисками, методологическая интеграция со смежными направлениями риск-ориентированного корпоративного управления.



Используемые лучшие практики и стандарты:

- ▶ Basel II.
- ▶ Risk IT.
- ▶ BS 25999.
- ▶ BS 25777.
- ▶ COSO ERM.
- ▶ COBIT.

Служба Service Desk

В качестве расширения услуги дополнительно могут быть выполнены следующие работы:

- ▶ Сбор и формализация требований к ИС, обеспечивающей автоматизацию функций Service Desk.
- ▶ Постановка задач на разработку/доработку ИС Service Desk.
- ▶ Обзор рынка и анализ соответствия ИС Service Desk.
- ▶ Доработка/настройка выбранной ИС Service Desk.
- ▶ Внедрение ИС Service Desk.
- ▶ Тиражирование ИС Service Desk в филиалы Заказчика.

В рамках услуги осуществляется разработка и внедрение процессов управления и развития ИТ на основе сервисного подхода (ITIL/ITSM). В соответствии со спецификой деятельности компании разрабатываются следующий пакет документов:

- ▶ Методика предоставления ИТ-сервисов.
- ▶ Методика формирования и предоставления управленческой отчетности по службе Service Desk.
- ▶ Методика оценки себестоимости ИТ-сервисов.
- ▶ Положение о службе Service Desk.
- ▶ Каталог услуг.
- ▶ Соглашение об уровне обслуживания (SLA).
- ▶ Стандартные запросы на обслуживание.
- ▶ Регламенты, инструкции, шаблоны службы Service Desk.

Достижимые результаты при внедрении подхода ITSM:

- ▶ Соответствие ИТ-сервисов текущим и будущим потребностям бизнеса и клиентов.
- ▶ Улучшение качества предоставляемых ИТ-сервисов и эффективности ИТ-поддержки.
- ▶ Повышение проактивности работы ИТ-службы.
- ▶ Повышение удовлетворенности пользователей и их эффективности при использовании ИТ-сервисов.
- ▶ Снижение негативного воздействия сбоев в работе ИТ-систем на бизнес-процессы и работу пользователей.
- ▶ Снижение числа повторных сбоев.
- ▶ Снижение трудозатрат на обработку обращений пользователей и устранение сбоев.
- ▶ Рациональное использование ресурсов при обработке обращений за счет более равномерной нагрузки ИТ-специалистов и увеличения доли обращений пользователей, решенных менее квалифицированными ИТ-специалистами.
- ▶ Повышение прозрачности и управляемости деятельности по эксплуатации ИТ-систем и поддержке пользователей.
- ▶ Накопление знаний и уменьшение зависимости от ключевого персонала.



Используемые лучшие практики и стандарты:

- ▶ ITIL/ITSM.
- ▶ ISO/IEC 20000.

При разработке/адаптации методики обеспечения ИБ выполняются следующие работы:

- ▶ Классификация данных.

В рамках услуги могут быть разработаны следующие политики, регламенты и процедуры ИБ.

- ▶ Положение о защите информационных ресурсов от несанкционированного доступа.

- ▶ Положение об антивирусной защите.

- ▶ Положение о защите конфиденциальной информации.

- ▶ Порядок обеспечения ИБ при работе пользователей в корпоративной сети.

- ▶ Порядок обеспечения ИБ удаленного доступа к ресурсам корпоративной сети.

- ▶ Порядок обеспечения ИБ при взаимодействии с сетью Интернет.

- ▶ Порядок обеспечения ИБ при использовании электронной почты.

- ▶ Порядок обеспечения ИБ при использовании устройств с беспроводной связью

- ▶ Порядок обеспечения ИБ платежных систем

- ▶ Порядок обеспечения ИБ при заключении договоров со сторонними организациями.

- ▶ Порядок обеспечения ИБ при найме и работе с персоналом.

- ▶ Порядок управления доступом к прикладным системам.

- ▶ Порядок управления учетными записями.

- ▶ Порядок использования СКЗИ.

- ▶ Порядок работы с цифровыми носителями конфиденциальной информации.



Используемые лучшие практики и стандарты:

- ▶ СТО БР ИББС
- ▶ ФЗ-152 (Федеральный закон)
- ▶ ISO 27000
- ▶ COBIT

О компании ОТР

ОТР (ООО “Организационно-технологические решения 2000”) – ведущая российская консалтинговая компания в сфере информационных технологий и системной интеграции, специализирующаяся на предоставлении комплексных ИТ-решений для финансовых организаций, государственных структур и промышленных предприятий.

Компания ОТР является широкопрофильным системным интегратором, оказывающим широкий спектр комплексных услуг – от сбора требований до сопровождения ИС.

В ОТР существует система адаптации международных отраслевых стандартов (PMBoK, ITIL, COBIT, ISO 9001) для их успешного использования в работе с Заказчиками.

Система менеджмента качества компании ОТР соответствует требованиям международного стандарта ISO 9001:2000.



Контактная информация по услуге

Руководитель практики ИТ-консалтинга
Правильщиков Максим Павлович

Тел: +7 (495) 222-59-05

E-mail: ITC@otr.ru

Сайт: www.otr.ru

