МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ
УНИВЕРСИТЕТ им. А. И. ГЕРЦЕНА»

**ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И
ТЕХНОЛОГИЧЕСКОГО ОБРАЗОВАНИЯ**
Кафедра информационных технологий и электронного обучения

Основная профессиональная образовательная программа
Направление подготовки 09.03.01 Информатика и вычислительная техника
Направленность (профиль) «Технологии разработки программного обеспечения»
форма обучения – очная

Реферат

«Управление и методологии аудита информационных технологий»

Обучающегося 3 курса
Войтенко Игоря Александровича

Научный руководитель:
Кандидат педагогических наук,
доцент кафедры ИТиЭО
Атаян Ануш Михайловна

Санкт-Петербург
2021

Оглавление

Введение

На сегодняшний день информационные технологии становятся важной неотъемлемой частью любого предприятия. Для большинства предприятий, это не только способ автоматизации каких-либо операций, а также эффективный инструмент в конкуренции. Современные информационные технологии быстро адаптируются к новым потребностям предприятия.

С каждым годом сфера информационных технологий становится все более сложной. Их внедрение на предприятии является сложным и трудоемким процессом, на который приходится тратить достаточно большое количество времени и сил, но не в каждой компании могут позволить такие затраты. При этом соответствующий эффект предприятия не всегда получают, если сравнивать затраты, выполненные работы и полученный результат такой деятельности. Именно поэтому должен проводиться аудит информационных технологий.

Цель работы: рассмотреть методологии аудита информационных технологий (информационных систем).

Актуальность: как было сказано выше, информационные технологии быстрыми шагами внедряются на различные предприятия поэтому, чтобы минимизировать риски для бизнеса, в процессе аудита можно выявить те места инфраструктуры информационных систем, которые могут повлечь за собой эти риски.

Основная часть

Основные цели проведения аудита ИТ

- Оценить эффективность расходуемого на ИТ-задачи бюджета (включает в себя анализ затрат на зарплаты специалистов, капитальных затрат на оборудование, переменных затрат на лицензии, подписки в сервисах, хостинги, сервера и так далее);
- Оценить эффективность работы ИТ-отдела, а также общий уровень подготовки кадров;
- Определить места в инфраструктуре и бизнес-процессах, где ИТ-системы используются недостаточно эффективно, выработать рекомендации по повышению эффективности, перераспределению нагрузки;
- Оценить работу систем и процессов, которые обеспечивают безопасность данных компании;
- Оценить риски для информационных активов компании, определить методы минимизации этих рисков;
- Обеспечить, чтобы все связанные с ИТ-системой процессы соответствовали законам и стандартам отрасли.

Как было сказано выше, в процессе аудита можно выявить те места инфраструктуры информационных систем, которые могут повлечь за собой серию рисков для бизнеса. Также проводится оценка бизнес процессов и рабочей информации, проверка эффективности для деятельности компании. Важно понимать, что у руководства компании появятся доказательства, позволяющие понять целесообразность вносимых изменений.

Аудит ИТ требуется

- У вас уже есть свидетельства того, что ИТ-инфраструктура работает плохо, в ней есть слабые места.
- Глобально меняется структура компании — например, появились новые подразделения. Требуется аудит деятельности, чтобы решить, что оставить как есть, что нужно добавить, от чего, возможно, отказаться.

Это поможет принять решения о централизации определенных сервисов, стандартизации оборудования, общему снижению рисков и удобству администрирования.

- У компании поменялись владельцы или топ-менеджмент и новому руководству необходима актуальная информация о состоянии ИТ-инфраструктуры, нужно пройти аудит.
- Готовится внедрение новой для компании информационной системы или технологии, к примеру, ERP или CRM-системы, системы документооборота, в таком случае понадобится аудит ИТ.

Порядок подготовки и проведения ИТ-аудита

При проведении аудита информационных технологий можно выделить два основных этапа – это планирование ИТ аудита и проведение ИТ аудита. В работы, которые входят в планирование ИТ аудита, можно включить анализ структуры различных бизнес процессов, платформы информационных систем, структуры ролей, распределения ответственности, бизнес-рисков и бизнес-стратегий. Кроме того, на данном этапе происходит идентификация ИТ-рисков, проводится оценка уровня контроля проверяемых бизнес-процессов. И на основе полученной информации выбираются объекты ИТ аудита. Дополнительно на данном этапе составляется план ИТ аудита, подбирается оптимальная методика ИТ аудита. И только после этого выполняются все необходимые работы, связанные с выполнением поставленных задач.

Благодаря деятельности профессионалов в сфере ИТ аудита идентифицируются имеющиеся механизмы управления в сфере ИТ аудита, происходит документирование всех процедур, связанных со сбором и анализом информации. Также в процессе проведения ИТ аудита информационных систем выполняется оценка эффективности имеющихся механизмов управления при выполнении поставленных задач. Кроме того, проводится подробное тестирование, позволяющее выполнить в дальнейшем корректирующие действия для обеспечения оптимального состояния системы управления ИТ.

Принципы проведения аудита

- Целостность. Является основой профессионализма. Аудиторам и лицу, осуществляющему управление программой аудита, следует: осуществлять свою работу честно, старательно и ответственно; выявлять все применимые правовые требования и действовать в соответствии с ними; демонстрировать свою компетентность при выполнении своей работы; осуществлять свою работу беспристрастно, т.е. сохранять справедливость и объективность в отношении всего, с чем приходится иметь дело; быть чувствительными к любым воздействиям, которые, как можно ожидать, окажут давление на выработку суждений при проведении аудита.
- Беспристрастное представление результатов. Является обязательством представлять правдивые и точные отчеты. Результатам аудита, заключениям по аудиту и отчетам об аудитах следует правдиво и точно отражать деятельность по проведению аудитов. Существенные препятствия, встретившиеся в ходе аудита, а также неразрешенные расходящиеся мнения и разногласия между командой по аудиту и аудитируемой организацией следует отражать в отчете. Коммуникации следует быть честной, точной, объективной, своевременной, понятной и полной.
- Надлежащая профессиональная тщательность. Означает приложение усердия (прилежания) и проявление рассудительности при проведении аудита. Аудиторам следует проявлять заботу о тщательности, которая должна соответствовать важности выполняемого ими задания и доверию, оказываемому им заказчиком аудита и другими заинтересованными сторонами. Важным фактором осуществления их деятельности с надлежащей профессиональной тщательностью является наличие способности вырабатывать здравые суждения во всех ситуациях, возникающих во время аудита.

- Конфиденциальность. Означает обеспечение безопасности полученной информации. Аудиторам следует проявлять осторожность в использовании информации, запрашиваемой в связи с осуществляемой ими деятельностью, и защищать ее. Информацию, полученную в ходе аудита, не следует использовать в целях получения выгоды для аудиторов или заказчика аудита или таким образом, который наносит ущерб законным интересам аудитируемой организации. Данный подход включает в себя должное обращение с "чувствительной" или конфиденциальной информацией.
- Независимость. Это основа беспристрастности при проведении аудита и объективности заключений по аудиту. Аудиторам, где это только возможно, следует быть независимыми от деятельности, которая будет подвергаться аудиту, и во всех случаях действовать таким образом, чтобы быть свободными от предвзятости и конфликта интересов. При проведении внутренних аудитов аудиторам следует быть независимыми от руководителей функциональных структур, подлежащих аудиту. Аудиторам следует сохранять объективность во время всего процесса аудита для обеспечения того, чтобы результаты аудита и заключения по аудиту были основаны только на свидетельствах аудита. Для малых организаций, возможно, будет достаточно того, чтобы внутренние аудиторы были полностью независимыми от деятельности, подвергаемой аудиту, но при этом следует приложить все усилия, чтобы исключить предвзятость и обеспечить объективность.
- Подход, основанный на свидетельствах. Является разумным способом получения надежных и воспроизводимых заключений по аудиту в процессе систематически проводимых аудитов. Свидетельствам аудита следует быть верифицируемыми. Они в общем случае будут базироваться на выборках доступной (полученной в распоряжение) информации, поскольку аудит проводится в ограниченный период

времени и с ограниченными ресурсами. Следует использовать соответствующие (уместные, подходящие) выборки примеров, поскольку это сильно влияет на доверие к заключениям по аудиту.

Методология проведения ИТ-аудита

При проведении ИТ аудита используются международные и внутренние стандарты ИТ аудита. Основные международные стандарты и лучшие практики проведения аудита информационных технологий – это ГОСТ Р ИСО 19011-2003, IS Standards, COBIT 4.1, федеральный стандарт аудиторской деятельности №15, ISO 27001:2005 и многие другие стандарты. При этом такие стандарты позволяют охватить только ключевые моменты проведения аудита. Для реализации дополнительных задач могут быть использованы другие стандарты.

В процессе проведения аудита, который дает возможность оценить текущее состояние информационных систем компании, механизмов управления и бизнес-процессов, выполняется следующий алгоритм работ.

В первую очередь формируется ориентированная на риски программа аудита. Во-вторых, проводится самооценка и интервью. Далее проводятся наблюдения за деятельностью, приводятся документальные доказательства. После этого происходит оценка уровня состоятельности ИТ процессов, а также оценка остаточного уровня рисков, связанных с такими процессами. В методологии ИТ аудита очень важна последовательность выполнения работ, так как от этого зависит полученный результат. Результат ИТ аудита – составление выводов и рекомендаций, аудиторского отчета, презентация заказчику полученных материалов.

COBIT

COBIT является единым подходом к сбору, анализу информации, подготовке выводов и заключений на всех этапах управления, контроля и аудита ИТ, предоставляющих возможность сравнения существующих ИТ-процессов с лучшими практиками, в том числе отраслевыми. COBIT разработан в форме открытого стандарта и регулярно принимается во многих государствах в виде

модели управления и контроля для введения и реализации эффективного управления ИТ.

Если рассматривать COBIT в области управления информационными технологиями, то целями являются ориентирование ИТ на нужды бизнеса, использование ИТ для максимизации выгоды для бизнеса, рациональное использование ИТ-ресурсов и управление ИТ-рисками.

COBIT может помочь предприятиям в достижении следующих целей:

- организовать процессы управления информационными технологиями на базе передового опыта и с ориентацией на нужды бизнеса;
- достичь поставленных бизнес-целей, в том числе соответствия стандартам;
- установить четкие и аргументированные цели бизнес-процессов, подходящие бизнес-целям предприятия, и предоставить средства измерения прогресса на пути их достижения;
- обеспечить эффективное регулирование информационных технологий и контроль на уровне бизнес-процессов, возможность ИТ-подразделения осознать, насколько оно исполняет требования к информационным технологиям, поставленные государственными или внешними регулирующими органами.

Основными объектами COBIT являются:

- ресурсы;
- критерии оценки;
- инструменты.

В качестве критериев оценки информации в COBIT отметим:

- полезность (соответствие требованиям потребителя, использующего информацию для выполнения своей задачи);
- эффективность (актуальность информации, соответствующего бизнес процесса, гарантия своевременного и регулярного получения

правильной информации. Информация считается эффективной, если она соответствует требованиям потребителя, ее нетрудно получить и использовать);

- достоверность (правдивость информации. Данный критерий скорее связан с восприятием пользователя, чем с фактической точностью);
- доступность (обеспечение доступности информации с помощью оптимального использования ресурсов);
- конфиденциальность (обеспечение защиты информации от неавторизованного ознакомления);
- целостность (точность, полнота и достоверность информации в соответствии с требованиями бизнеса);
- соответствие требованиям (соответствие законам, правилам и договорным обязательствам).

В методологии COBIT присутствуют взаимосвязанные инструменты для ответа на вышеизложенные вопросы, такие как модель зрелости, критические факторы успеха, ключевые индикаторы цели и ключевые показатели результата.

Модель зрелости предназначена для организации эффективного управления методом определения ключевых действий, которые показывают, что нужно сделать для достижения необходимого уровня зрелости, и содержат способы контроля над правильностью исполнения основных ИТ-процессов и методов их измерения. Всего существует 6 уровней зрелости процессов:

- уровень 5 – оптимизированные;
- уровень 4 – предсказуемые;
- уровень 3 – налаженные;
- уровень 2 – управляемые;
- уровень 1 – выполняемые;
- уровень 0 – неполные.

COBIT описывает жизненный цикл информационных технологий с помощью четырех групп, так называемых доменов процессов:

- планирование и организация (PO) (определяет направления в отношении внедрения решений (AI) и обеспечение услуг);
- приобретение и внедрение (AI) (обеспечивает внедрение решений и оказание услуг на их основе);
- эксплуатация и сопровождение (DS) (представляет решения и делает их применимыми для конечных пользователей);
- мониторинг и оценка (ME) (выполняет надзор за всеми процессами, чтобы убедиться в продвижении в верном направлении).

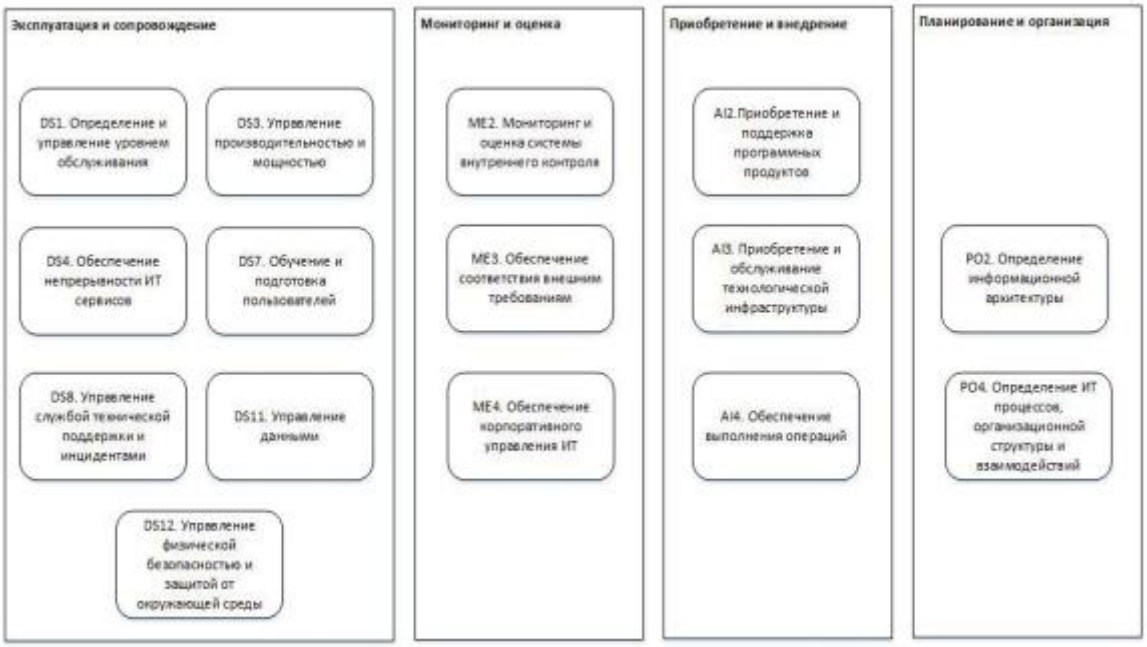
COBIT является документом высокого уровня, при внедрении его необходимо применение специфических стандартов. COBIT представляет собой руководство, а не готовое решение, требует выполнения соотношения рисков, проектов и инфраструктуры информационных технологий на предприятии с учетом бизнес-целей предприятия.

Для эффективной реализации оценки зрелости бизнес-процессов как основного элемента внутреннего аудита по методологии COBIT важно оценить существующее программное обеспечение. На рынке имеется несколько программных продуктов для реализации управления ИТ:

- Meycor COBIT Suit;
- RSAM GRC;
- Easy2comply GRC;
- GRC&Audit Enterprise Suit;
- ProcessGene Suite Plug-In.

Данные программные продукты представляют собой системы GRC (Governance, Risk management, and Compliance), включающие управление предприятием, управление рисками и соответствие стандартам. В настоящее время существует ряд проблем, связанных с использованием подобных систем на российском рынке: слабый менеджмент организации;

отсутствие стабильных бизнес-процессов; отсутствие формализации бизнес-процессов, а также обработки нарушений и отклонений от стандартов.



Процессы в рамках методологии COBIT

ГОСТ Р ИСО 19011-2003

Настоящий стандарт содержит руководящие указания по принципам аудита, управлению программами аудита, проведению аудитов систем менеджмента качества и систем экологического менеджмента, а также по компетентности аудиторов для проведения этих аудитов.

Настоящий стандарт предназначен для организаций, которым необходимо проводить внутренние и/или внешние аудиты систем менеджмента качества и/или систем экологического менеджмента или управлять программами аудита.

ISO/IEC 27001

ISO/IEC 27001 — международный стандарт по информационной безопасности, разработанный совместно Международной организацией по стандартизации и Международной электротехнической комиссией. Подготовлен к выпуску подкомитетом SC27 Объединенного технического комитета JTC 1.

Стандарт содержит требования в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности(СМИБ)

Лучшие мировые практики в области управления информационной безопасностью описаны в международном стандарте на системы менеджмента информационной безопасности ISO/IEC 27001 (ISO 27001). ISO 27001 устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы.

Понятие «защиты информации» трактуется международным стандартом как обеспечение конфиденциальности, целостности и доступности информации. Основа стандарта ИСО 27001 — система управление рисками, связанными с информацией.

ISA

Международные стандарты аудита (ISA) - это профессиональные стандарты аудита финансовой информации. Эти стандарты издаются Международной федерацией бухгалтеров (IFAC) через Совет по международным стандартам аудита и подтверждения достоверности информации (IAASB). По словам Олунга М. (CAO - L), ISA направляет аудитора, чтобы повысить ценность задания, тем самым укрепляя доверие инвесторов.

Стандарты охватывают различные области аудита, включая соответствующие обязанности, планирование аудита, внутренний контроль, аудиторские доказательства, использование работы других экспертов, аудиторские заключения и аудиторские отчеты , а также стандарты для специализированных областей.

Заключение

Таким образом в работе мы рассмотрели аудит ИТ его цели, принципы, а также основные документы, которые регламентируют проведение аудита.

Кто заинтересован в проведении аудита? Прежде всего, это коммерческие или бюджетные организации и предприятия для обоснования инвестиций в ИС, системные интеграторы, ИТ компании для оценки влияния ИС на основной бизнес-процесс и расширения спектра предлагаемых услуг.

Для компаний, проводящих финансовый аудит — аудит ИС, дополнительная услуга, которая способна повысить рейтинг компании на рынке.

Генеральным подрядчикам работ будет интересна возможность оценить работу субподрядчиков в сфере ИТ.

А также проведение аудита ИС по стандарту CoBiT будет интересно любым предприятиям и организациям, имеющим или планирующим создание ИС и которые заинтересованы в получении ответов на вопросы, приведенные выше.

Аудит Информационных процессов позволяет руководителю:

- Оценить степень соответствия ИС требованиям бизнеса.
- Определить приоритеты основных ИТ-процессов.
- Выявить критически важные элементы ИТ.
- Выявить и оценить факторы риска.

Оценить степень защищенности компании от чрезвычайных происшествий и их последствий.

Создать план работ по устранению недостатков и разработать способы их устранения.

Руководитель организации, заказавший аудит ИТ у внешней аудиторской компании, должен понимать, что через полгода-год (в зависимости от динамики развития) ситуация в организации изменится, результаты аудита потеряют свою актуальность.

Если в этот момент не провести повторный аудит для сравнения с предыдущими результатами, то деньги, вложенные в "первый" аудит, можно считать потерянными и придется проводить "первичный" аудит заново.

Основным преимуществом регулярного проведения аудита является накопление знаний организации, создание собственной базы знаний, которая позволит быстро и достоверно ответить на большинство вопросов, возникающих в организации.

Источники

1. URL:https://en.wikipedia.org/wiki/Information_technology_audit (дата обращения: 22.12.2021).
2. URL:https://intuit.ru/studies/courses/4459/855/lecture/32609 (дата обращения: 22.12.2021).
3. URL:https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/russian/deloitte-it-audit.pdf (дата обращения: 22.12.2021).
4. URL:https://www.sk.kz/upload/iblock/33d/33d6d6158e36dbca8b170cf0924b83fb.pdf (дата обращения: 22.12.2021).
5. URL: https://auditfin.com/fin/2009/3/04_05/04_05%20.pdf (дата обращения: 22.12.2021).
6. URL: https://moluch.ru/archive/345/77632/ (дата обращения: 22.12.2021).
7. URL: https://www.itexpert.ru/rus/audit/itaudit/ (дата обращения: 22.12.2021).
8. URL: https://integrus.ru/blog/it-audit.html (дата обращения: 22.12.2021).
9. URL: https://intuit.ru/studies/courses/4459/855/lecture/32612?page=2 (дата обращения: 22.12.2021).
10. URL: https://cyberleninka.ru/article/n/provedenie-audita-informatsionnoy-sistemy-na-osnove-metodologii-cobit/viewer (дата обращения: 22.12.2021).
11. URL: https://ru.wikipedia.org/wiki/Cobit (дата обращения: 22.12.2021).
12. URL: https://helpit.me/articles/standarty-it-audita (дата обращения: 22.12.2021).
13. URL: https://docs.cntd.ru/document/1200034758 (дата обращения: 22.12.2021).
14. URL: https://en.wikipedia.org/wiki/International_Standards_on_Auditing (дата обращения: 22.12.2021).
15. URL: https://iso-management.com/iso-27001-2005/ (дата обращения: 22.12.2021).
16. URL:https://en.wikipedia.org/wiki/International_Standards_on_Auditing#:~:text=International%20Standards%20on%20Auditing%20(ISA,Assurance%20Standards%20Board%20(IAASB). (дата обращения: 22.12.2021).