УДК 338.27:338.242

Петров В.Ю., Тарасова Е.С.
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, e-mail: petrovvu2005@rambler.ru

ПОДХОДЫ К ПРОВЕДЕНИЮ ИТ-АУДИТА В МАЛОМ И СРЕДНЕМ БИЗНЕСЕ

Ключевые слова: информационная технология, аудит, ИТ-аудит, типы услуг ИТ-аудита, ключевые подходы проведения аудита, риски, оценка рисков.

Актуальность исследования обусловлена значительным ростом числа предприятий малого и среднего бизнеса и реализацией в них стратегии развития информационных технологий (ИТ) в современных условиях. Недостаточная отдача от ИТ наряду с высокими расходами на обслуживание ИТ-систем, приводит к таким решениям этих проблем как использование консалтинговых услуг и аудита. В связи с этим авторы выбрали такой предмет исследования как аудит, пути его проведения и некоторые проблемы, связанные с этим направлением. Помимо типов услуг проведения ИТ-аудита, в статье рассматриваются ключевые подходы к проведению аудита, идентификация, качественная и количественная оценка рисков по двум параметрам, даются рекомендации по временным рамкам и необходимости проведения оценок рисков и аудита, приводится алгоритм выявления необходимости проведения анализа рисков и определения величины потенциального ущерба от них. Авторы приводят некоторые методики и международные стандарты, которые рекомендованы для проведения аудита. Указывается, что без проведения аудита немыслимо успешное, адекватное, соответствующее современному законодательству функционирование предприятий.

Petrov V.Yu., Tarasova E.S.
St. Petersburg National Research University of Information Technologies, Mechanics And Optics, St. Petersburg, e-mail: petrovvu2005@rambler.ru

APPROACHES TO CARRYING OUT IT AUDIT IN SMALL AND MEDIUM BUSINESS

Keywords: information technology, audit, IT audit, types of services of IT audit, key approaches of carrying out audit, risks, risk assessment.

The relevance of a research is caused by significant growth in number of the enterprises of small and medium business and implementation of the strategy of development for the information technologies (IT) in them in modern conditions. Insufficient return from IT along with high expenses on service of IT systems, leads to such solutions of these problems as use of consulting services and audit. In this regard authors chose such object of research as audit, ways of its carrying out and some problems connected with this direction. Besides types of services of carrying out IT audit, in article key approaches to carrying out audit, identification, high-quality and quantitative risk assessment in two parameters are considered, recommendations about time frames and need of carrying out risk assessment and audit are made, the algorithm of detection of need of carrying out risk analysis and determination of size of potential damage from them is given. Authors give some techniques and the international standards which are recommended for carrying out audit. It is specified that without carrying out audit the successful, adequate, corresponding to the modern legislation functioning of the enterprises is impossible.

Современной тенденцией развития экономики, как и всей нашей жизни является эволюция, причем одним из основных ее направлений является информатизация. Практически все компании, учреждения, предприятия малого и среднего бизнеса, независимо вида деятельности, используют информационные технологии (ИТ). Для большинства из них ИТ является обеспечивающей частью основной деятельности, поэтому внедрение, использование, модификация этих технологий в управлении и развитии предприятий часто носит хаотичный характер. Хотя уровень грамотности персонала постоянно растет, тем не менее пробелы в знаниях у работников, их заторможенность в изучении нового материала, в результате нехватка квалификации и опыта у специалистов, ограниченные средства на приобретение нового оборудования и программного обеспечения приводит к несоответствию имеющихся информационных

технологий целям и задачам деятельности компании, частым ошибкам и сбоям в работе, а иногда к потери и утечки данных. Особенно эти проблемы наблюдаются в компаниях, относящихся к сектору малого и среднего бизнеса. Обусловлено это тем, что в данных компаниях, как правило, ИТ-специалистов гораздо меньше, и обычно они обеспечивают операционную деятельность компании, зачастую не задумываясь о соответствии ИТ бизнес-стратегии компании. Замечая недостаточную отдачу от ИТ наряду с высокими расходами на обслуживание ИТ-систем, руководители должны решать, как исправить указанные недостатки.

Помимо всего прочего, одним из вариантов решения указанной проблемы является использование консалтинговых услуг, аудита. Именно поэтому уже сегодня для российской ИТ-сферы характерен рост спроса на краткосрочные консалтинговые услуги, связанные с эффективностью ИТ в компании к которым относится и ИТ-аудит, что определяет актуальность рассматриваемой темы.

ИТ-аудит – это деятельность, направленная на оценку соответствия ИТ-инфраструктуры внутренним и внешним требованиям, которая может включать в себя инвентаризацию, исследование и анализ ИТ-инфраструктуры компании и предоставления рекомендаций для снижения рисков, связанных с ИТ [3]. Задачи, которые ставили авторы статьи сводятся к рассмотрению отдельных важных вопросов проведения аудита.

Согласно результатам исследования Института внутренних аудиторов (IIA), в 2017г. оценка эффективности использования ИТ в планах у 42% респондентов, 45% проводят ее в настоящий момент (против 26% в 2015 году). При этом абсолютное большинство компаний (92%) при проведении ИТ-аудитов привлекают внешних специалистов в области информационных систем и технологий [2].

Столь высокий процент привлечения внешних аудиторов может быть объяснен тем фактом, что для проведения ИТ-аудитов необходимо, чтобы в штате компании были специалисты, обладающие высоким уровнем ИТ-компетенций. Без наличия соответствующих специалистов проведение качественных проектов ИТ-аудита невозможно.

В самом общем случае проведение аудита можно свести к 5 этапам: планирование аудита, получение общего представления об ИТ процессах организации, анализ исков, тестирование контрольных процедур, составление аудиторского заключения [4]. В процессе выбора услуги ИТ-аудита представители малого и среднего бизнеса руководствуются, прежде всего, целями его проведения и имеющимся бюджетом. Задача же аудиторских компаний – предложить оптимальный вариант аудита, ориентируясь на потребности заказчика аудита.

Процедура ИТ-аудита, как правило, занимает от 2 недель до 2 месяцев, в зависимости от специфики компании и масштаба ее ИТ-инфраструктуры. Поэтому в начале проекта ИТ-аудита необходимо определить объекты аудита, оценить продолжительность и стоимость ИТ-аудита. Для этого аудиторскими компаниями производится сбор первичной информации об ИТ-инфраструктуре компании и организации в целом посредством анкетирования ответственных лиц компании заказчика. В анкеты, как правило, включаются вопросы об используемом оборудовании, программном обеспечении, ключевых ИТ-системах, информация об ИТ-подразделении и проблемах, связанных с ИТ.

На данный момент компании, предоставляющие услуги ИТ-аудита, в зависимости от объектов аудита и глубины их исследования, подразделяют его на несколько типов (таблица 1).

В проведении бизнеса и в процессе ИТ-аудита большинство компаний руководствуются наилучшим мировым опытом, изложенным в методологии менеджмента ITIL/ITSM, включающей две технологии, где один метод – IT Systems Management сконцентрирован на технологиях, другой – IT Service Management на услугах [5]; а также в международных стандартах: COBIT [9, 10], ISO 19011, ISO 20000 [6, 7] и др., которые реализуют разные подходы к проведению ИТ-аудита.

Таблица 1

Типы услуг ИТ-аудита

№ п/п	Наименование	Цель	Объекты аудита
1	Экспресс-аудит	оценка сложности ИТ-инфраструктуры, поиск проблемных мест, оценка оптимальности использования оборудования и правильности его функционирования	любой объект ИТ
2	Направленный ИТ-аудит	получение информации об отдельных элементах ИТ-инфраструктуры	любой объект ИТ-инфраструктуры (ПО, оборудование, локальная сеть, ИТ-подразделение), в зависимости от цели ИТ-аудита и требований заказчика
3	Комплексный ИТ-аудит	Полная проверка состояния ИТ инфраструктуры компании и создание глобального проекта по модернизации для достижения показателей эффективности – качества, быстродействия, экономичности и др.	ИТ-инфраструктура в целом
4	ИТ-обследование	Получение четкого представления о текущем состоянии ИТ-инфраструктуры	Оборудование и программное обеспечение
5	Технический аудит	Получение информации о соответствии информационной системы общепринятым стандартам и рекомендации по модернизации	Производительность систем и оборудования
6	Аудит ИТ-бизнес-процессов	Повышение эффективности и качества исполнения существующего бизнес-процесса	Техническая составляющая (системы и оборудование) + регламенты бизнес-процесса
7	Экспертная оценка	Определение целесообразности и эффективности затрат на реализацию ИТ-проектов, покупку оборудования и ИТ-услуг	Затраты на ИТ
8	Аудит ИТ-критерия	Оценка соответствия работы ИТ-инфраструктуры определенному критерию, например, критерию информационной безопасности	Совокупности элементов системы (как оборудования, так и ПО) в рамках оценки одного критерия

Подход к ИТ-аудиту определяет цель аудита, порядок сбора и состав собираемых данных, результат. На сегодняшний день выделяется несколько ключевых подходов к проведению аудита:

1. Комплаенс-подход, направленный на оценку полноты и правильности соблюдения разного рода внешних и внутренних требований – законов, стандартов, предписаний и т.д.

На данный момент комплаенс-подход используется при проведении аудита информационной безопасности, в частности при проверке соответствия требованиям Федерального закона № 152 «О персональных данных». Также комплаенс-подход применяется при проверке лицензионной чистоты программного обеспечения.

На сегодняшний день комплаенс-подход к аудиту подразделяется на два типа:

− поверхностный комплаенс-подход, который подразумевает поиск несоответствий внутренним и внешним требованиями и предоставлению рекомендаций по их исправлению;

− углубленный комплаенс-подход, который включает в себя выявление фактов несоответствия требованиям, описание факторов риска, оценку последствий возникновения риска и выход из сложившейся ситуации.

2. Операционный подход, основной задачей которого является выявление факторов, препятствующих достижению бизнес-целей компании. Данный подход способствует оценке соответствия существующей ИТ-инфраструктуры

бизнес-целям и требованиям компании в функциональном и практическом плане.

3. Риск-ориентированный подход, направленный на выявление факторов риска, связанных с ИТ, и поиск способов нивелирования негативного воздействия в случае их наступления [1].

Во всех случаях проведения аудита важным моментом является оценка различного рода рисков. Под ИТ-риском понимается вероятность возникновения негативных событий (убытков, ущерба), связанных с использованием компанией информационных технологий. К ИТ-рискам относят риски информационной безопасности (утечки и потери данных), риски недостижения целей применения ИТ для повышения эффективности основной деятельности и пр.

Исследования и практика проведения аудита информационных систем показывают, что правомерность вопроса о необходимости исследовании рисков на этапах по управлению этими рисками можно оценить исходя из алгоритма, представленного на рисунке 1 [3].

Конечно, тот вариант, когда ущерба не предвидится и рисков нет – фантастика. Как правило, при внедрении ИС всегда присутствует риск и потенциальный ущерб. Поэтому сначала оценив их, следует решить, нужна ли защита информации и ИС от угроз того или другого типа. В соответствии с этим алгоритмом, определяя величину риска и ущерба, следует учитывать и вероятностные характеристики уязвимостей и угроз.

Поскольку идентификация и оценка рисков – трудоемкий и длительный процесс, при использовании риск-ориентированного подхода чаще всего производится выборочная проверка ИТ-инфраструктуры, в основном в «критических точках» – там, где риски выше; области с низкими рисками исключаются из проверки, тем самым сокращается затраченное время.

Процесс управления рисками включает в себя идентификацию ИТ-рисков, количественную и качественную оценку выделенных рисков, определение тактики реагирования на риски, мониторинг и контроль рисков.

Первым этапом в построении риск-ориентированного подхода к аудиту ИТ является описание бизнес-процессов, связанных с ИТ. Во избежание чрезмерной детализации предлагается описывать ИТ-процессы, имеющие критическое значения для деятельности компании в целом.

Например, руководствуясь рекомендациями стандарта COBIT, к таким процессам, присущим любой организации, независимо от ее размера, индустрии и специфики деятельности, отнесены следующие [10]:

− PO4. Формализация ИТ-процессов и взаимоотношений с бизнесом.

− PO5. Управление инвестициями в ИТ.

− PO6. Согласованное управление целями и задачами.

− PO9. Оценка и управление рисками ИТ.

− AI6. Управление изменениями.

− AI7. Установка и утверждение решений и изменений.

− DS5. Обеспечение безопасности систем.

− DS8. Управление службой технической поддержки и инцидентами.

− DS11. Управление данными.

− DS12. Управление физической безопасностью и защита от воздействия окружающей среды.

− DS13. Управление операциями по эксплуатации систем.

− ME4. Обеспечение корпоративного управления ИТ.

Следующим шагом проектирования риск-ориентированного подхода к аудиту ИТ может, как вариант, является построение карты рисков. На данном этапе необходимо описать все ИТ-риски, присущие организации, оценить степень влияния и вероятность выявленных рисков [8].

Для структурирования рисков можно разбивать их на категории, например, технологические риски, бизнес-риски, риски, связанные с ИТ-персоналом, риски информационной безопасности и др.

Оценка рисков включает в себя оценку воздействия риска на деятельность компании, и рассчитывается по формуле:

$$Риск = Вероятность\_происшествия \times \times Цена\_потери$$

Такие вычисления возможны, если переменные являются количественными величинами. Тогда риск – это оценка математического ожидания потерь и может производиться как в финансовых показателях.

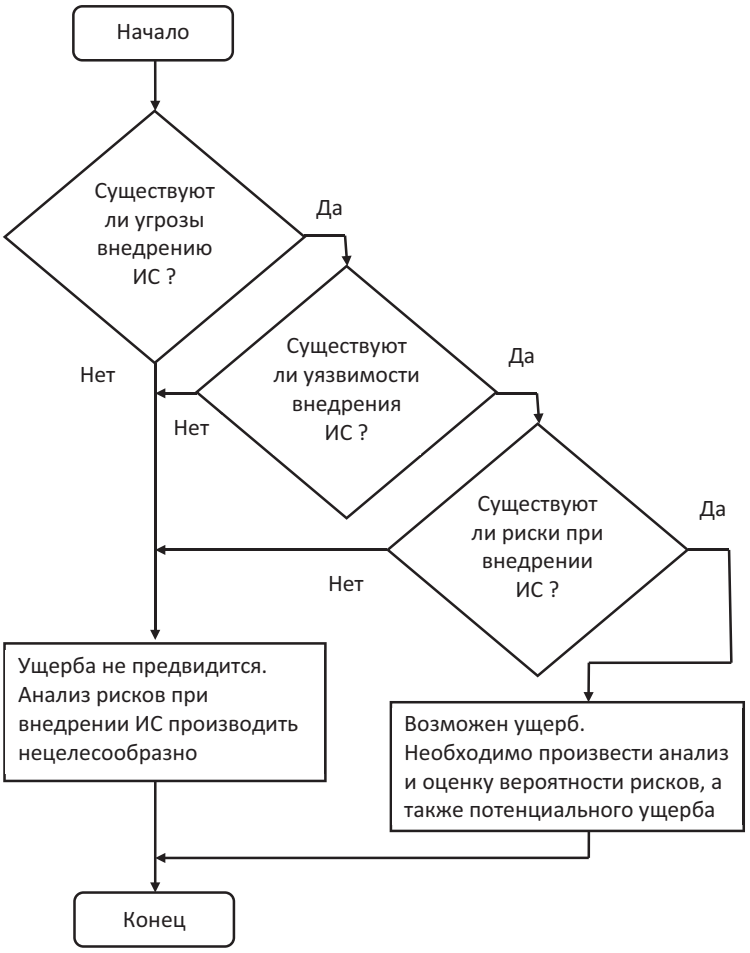

Рис. 1. Алгоритм выявления необходимости проведения анализа рисков и определения величины потенциального ущерба

Но наиболее часто переменные являются качественными величинами, и так как в этом случае операция умножения в явном виде не определена, приведенная формула использоваться не может. Результат в этом случае получают в качественных показателях, а каждая компания в процессе разработки и внедрения риск-ориентированного подхода к ИТ-аудиту самостоятельно определяет количество уровней влияния рисков и их значение на компанию (таблица 2).

В процессе разработки и внедрения риск-ориентированного подхода в компании необходимо также разработать шкалу вероятности появления риска (таблица 3).

Стоит отметить, что частота появления ИТ-рисков связана с уровнем зрелости ИТ в компании. Именно поэтому шкала вероятности появления риска должна разрабатываться индивидуально для каждой компании.

Для окончательного расчета величины ИТ-риска, результаты оценки влияния и вероятности перемножаются и отражаются на карте рисков, представленной на рисунке 2.

По результатам проведенной оценки происходит ранжирование рисков, на основании чего может быть предоставлены рекомендации о частоте проведения анализа рисков. Например: для рисков, попавших в сектор с низким уровнем, их проверка и анализ может осуществляться раз в 3 года; для рисков, попавших в сектор со средним уровнем, проверка и анализ может осуществляться раз в 2 года; для рисков, попавших в сектор с высоким уровнем, проверка и анализ должны проводится раз в год.

Таблица 2

Пример оценки влияния риска на деятельность компании

Ранг	Значение	Финансовое влияние	Нефинансовое влияние
1	Минимальное	Отсутствует	Отсутствие последствий
2	Среднее	До удерживающей способности	Последствия риска незначительны и устранимы в течение 24 часов
3	Высокое	Потеря до 50% доходности	Последствия риска значительны, но устранимы в течение дня
4	Критическое	До полной потери доходности	Последствия значительные, но могут быть исправлены до определенной степени
5	Катастрофическое	Полная потеря доходности	Последствия значительные, и не могут быть исправлены

Таблица 3

Пример оценки вероятности появления риска

Ранг	Значение	Вероятность появления риска
1	Очень редко	Инцидент возникает раз в 5 лет
2	Редко	Инцидент возникает раз в 3 года
3	Время от времени	Инцидент возникает раз в год
4	Часто	Инцидент возникает раз в полгода
5	Очень часто	Инцидент возникает раз в месяц или чаще

		Влияние риска на деятельность компании				
		Минимальное	**Среднее**	**Высокое**	**Критическое**	**Катастрофическое**
Вероятность появления риска	**Очень редко**	Низкий риск	Низкий риск	Низкий риск	Низкий риск	Средний риск
	Редко	Низкий риск	Низкий риск	Средний риск	Средний риск	Средний риск
	Время от времени	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
	Часто	Низкий риск	Средний риск	Средний риск	Высокий риск	Высокий риск
	Очень часто	Средний риск	Средний риск	Высокий риск	Высокий риск	Высокий риск

Рис. 2. Пример карты рисков для двух параметров

Кроме этого, для рисков, имеющих средний и высокий уровень, необходимо разработать меры по их снижению. Хранить данную информацию можно в матрице рисков и контрольных процедур, включающей в себя:

1. Номер и наименование процесса.
2. Номер и наименование риска.
3. Присвоенный на карте рисков ранг.
4. Номер и наименование контроля – описание мер для снижения риска.
5. Тип контроля – выявляющий или предотвращающий.
6. Частота контроля.
7. Владелец контроля – ответственное лицо по проведению мер для снижения риска.

На основании разработанной матрицы рисков и контрольных процедур заводят Журнал регистрации ИТ-рисков, по которому следует отслеживать текущий уровень управления рисками и предпринятые меры для снижения рисков. Журнал рисков может включать в себя следующие поля:

− наименование риска;

− последствия риска;

− текущий ранг риска (согласно карте рисков) и дата его присвоения;

− ответственный за предотвращение последствий риска;

− предпринятые меры по устранению риска;

− необходимость дополнительных мер;

− сроки устранения риска;

− последствия риска;

− необходимость изменения ранга риска (в случае пересмотра уровня влияния риска на деятельность компании или изменения частоты появления риска).

На основе данных Журнала регистрации ИТ-рисков может происходить обновление документов, регламентирующих управление ИТ-рисками.

Практика показывает то, что руководителям предприятий и служащим проблемы возникающие в бизнесе зачастую трудно видеть из-за того, что они возникли в результате их же действий. Поэтому если предприятие проигрывает в конкурентной борьбе, уменьшается приток капитала, возникают непредвиденные трудноразрешимые ситуации, значит на предприятии что-то идет не так, а руководитель и служащие чего-то не видят. Необходим непредвзятый взгляд со стороны, то есть проведение аудита.

В крайнем случае частота его проведения должна определяться, например, по карте рисков, а компоненты должны соответствовать международным стандартам и основным задачам бизнеса. В зависимости от задач бизнеса компания может:

− **проводить аудит системы управления**, а именно: анализ сферы ответственности ключевых сотрудников, устранение дублирования функций и функциональных провалов, анализ эффективности планирования и контроля сроков и др.

− **проводить аудит отдела продаж**: структуру клиентской базы, анализ процессов удержания клиентов, уменьшения оттока, стратегии создания лояльности, поиск способов повышения среднего чека, анализ цепочки обслуживания, поиск и устранение точек потерь клиентов и т.д.

− **проводить финансовый аудит: п**роверка финансовая безопасность бизнеса, проверка бухгалтерский и управленческий учет, контроль денежных потоков

Любой подход к проведению аудита бесспорно снимет часть ответственности с предпринимателей и наладит производственный цикл. Глубина же и качество аудита определяется финансовыми возможностями предприятия.

Библиографический список

1. Смирнов С.Б., Кривцова И.Е., Петров В.Ю. Основы экономики защиты информации. – Германия: Изд-во LAP LAMBERT Academic Publishing, 2015. – 256 с. [Электронный ресурс]. – URL: https://www/.livelib.ru/book/1001425602/ (дата обращения: 02.12.2018).

2. Проекты внешнего аудита ИТ и безопасности. Tadviser [Электронный ресурс]. – URL: http://www.tadviser.ru/ (дата обращения: 02.12.2018).

3. Лукьянова Е.Е., Петров В.Ю. Анализ методов проведения аудита // Труды XLII научной и учебно-методической конференции НИУ ИТМО «Актуальные проблемы менеджмента в России на современном этапе развития теории и практики управления сложными социально-экономическими системами и процессами. СПб НИУ ИТМО, ГФ, 2013.

4. Стандарты ITIL/ITSM/. BzBook.ru/ [Электронный ресурс]. – URL: http://bzbook.ru/Informaczionnye-tekhnologii-i-upravlenie-predpriyatiem.74.html/ (дата обращения: 02.12.2018).

5. Стандарт CobiT. Управление и аудит информационных технологий. Особенности проведения внешнего аудита. ИТ Jet Info // Информационный бюллетень. – 2003. – № 1(116).

6. Обзор стандарта COBIT (Control Objectives for Information and related Technology) V. 4.1. Методология, процессы, критерии, внедрение Cobit. IT Expert. Training and examination center/ 2019 г. [Электронный ресурс]. – URL: https://www.itexpert.ru/rus/biblio/cobit/ (дата обращения: 12.01.2019).

7. ГОСТ Р ИСО/МЭК 20000-1-2010. Информационная технология (ИТ). Менеджмент услуг [Электронный ресурс]. – URL: https://steptosleep.ru/ (дата обращения: 02.12.2018).

8. Международный стандарт. ISO 19011:2011 [Электронный ресурс]. – URL: http://iso-management.com/wp-content/uploads/2015/06/ISO-1901120111.pdf (дата обращения: 02.12.2018).

9. Крышкин О. Настольная книга по внутреннему аудиту. Риски и бизнес-процессы. – М.: Альпина Паблишер, 2015. – 600 с.

10. Оценка рисков по двум факторам [Электронный ресурс]. – URL: https://poisk-ru.ru/s32486t7.html (дата обращения: 02.01.2019).