УДК 007

ИНФОРМАЦИОННЫЙ АУДИТ. УПРАВЛЕНИЕ ИТ-РИСКОМ

Степура М.А.

Студентка 3 курса Института экономики и управления

ФГБОУ ВО «Бурятский государственный университет»,

Россия, г. Улан-Удэ.

Аннотация: Так как организации все больше становятся зависимыми от информационных технологий, им необходимо проводить ИТ аудит с целью оценки ИТ-инфраструктуры. Данная статья посвящена процессу информационного аудита, в ней определены его понятие, этапы проведения, методологическая основа и его значение. А также описаны способы управления ИТ-рисками.

Ключевые слова: информационные технологии, ИТ-инфраструктура, информационный аудит, ИТ-риски, управление ИТ-рисками, стандарты аудита.

INFORMATION AUDIT. MANAGEMENT OF IT-RISK

Stepura M. A.

student of the 3rd year of the Institute of Economics and Management,

Buryat state University,

Russia, Ulan-Ude.

Abstract: Since organizations are increasingly dependent on information technology, they need to conduct an it audit in order to assess the IT-infrastructure. This article is devoted to the process of information audit, it defines its concept, stages, methodological basis and its value. And also describes how to manage IT risks.

Keywords: information technologies, IT-infrastructure, information audit, IT-risks, IT-risk management, audit standards.

В современных условиях Информационные технологии (ИТ) являются эффективным способом воздействия на процессы организации. Их используют в управленческой деятельности: стратегическом управлении, управлении финансами, качеством продукции и услуг и др. Внедрение Информационных систем (ИС) и ИТ в деятельность компаний приносит большую пользу, например, автоматизируют и оптимизируют бизнес-процессы организации. Но неправильное их использование может стать причиной рисков, которые могут привести к возникновению у компании значительных убытков, а также к минимизации эффективности использования внедренных технологий. Для этого используют IT-аудит, который дает возможность выявить риски внедрения и эксплуатации ИТ, оценить эффективность системы ИТ и определить способы их совершенствования.

Информация является важным ресурсом для деятельности компаний и именно от нее, главным образом, зависит стратегия компании, ее положение на рынке, эффективность ее функционирования и многое другое. Компании имеют большую зависимость от информации и информационных технологий. И так как факторы, влияющие на ИТ, могут неблагоприятно влиять на происходящие бизнес-процессы, необходимо уменьшить влияние этих факторов во избежание рисков.

Под информационным риском понимают любой риск, который связан с использованием ИТ; это вероятность того, что уязвимость системы может быть использована для неблагоприятного воздействия на организацию. Для предупреждения и измерения таких рисков необходимо проводить ИТ-аудит.

ИТ-рисками могут быть не только проблемы, связанные с информационной безопасностью (хакерские атаки, хищение информации,

вирусы и так далее), но и такие проблемы как не достижение целей применения ИТ. Информационные технологии могут не соответствовать потребностям бизнеса или не соответствовать бизнес-стратегии и планам организации. Также риском может быть потеря определенных частей ИТ-инфраструктуры, что приведет к сбою осуществления бизнес-процессов в организации. Однако ключевым объектом аудита являются ИТ-процессы. В процессе проведения аудита оценивают ИТ-систему, которая представляет собой совокупность ИТ-процессов.

Понятие ИТ аудит в России появилось недавно. Аудит информационных технологий (информационный аудит) проводят с целью систематизации ИТ-процессов и получения точной информации для оценки ИТ и принятия решений по управлению. Целью аудита также является модернизация системы контроля за ИТ. ИТ-аудит позволяет обнаружить узкие места в ИТ-инфраструктуре, что дает возможность компании принять меры, по устранению ИТ-рисков. Результатом аудита является определение эффективности использования ресурсов и рекомендаций по повышению его эффективности.

Существует два подхода к проведению ИТ-аудита:

1. Стандартный подход. Его используют для комплексной оценки основных ИТ-процессов, которые свойственны любой организации.

2. Расширенный подход. Этот подход используют компании, которые в большей степени зависят от информации и информационных технологий. К таким компаниям можно отнести финансовые институты, телекоммуникационные или ИТ-компании.

Процесс информационного аудита состоит из нескольких этапов. На первом этапе необходимо разработать детальный план обследования. На этом этапе анализируются бизнес-процессы и их структура, ИС, бизнес-стратегии и бизнес-риски. Определяются ИТ-риски, производится оценка контроля бизнес-процессов. Результатом данного этапа является выбор объектов исследования,

то есть выделение тех ИТ-процессов и ресурсов, которые требуют анализа, оценки и контроля.

На втором этапе проводится сам ИТ-аудит. Собирается и проводится первичный анализ имеющейся информации, производится оценка существующих механизмов управления. Проходит проверка соответствия реально существующих механизмов с механизмами управления, необходимыми для решения задач, с его целевым уровнем. Последней составляющей этого этапа является подробное тестирование для нахождения узких мест и их устранения с помощью корректировки системы управления ИТ, формируется итоговая оценка.

Результатом проведения ИТ-аудита являются оценка текущего состояния и разработанные рекомендации по совершенствованию ИТ-инфраструктуры предприятия.

Для того чтобы организации могли выполнить свою миссию, необходимо управлять рисками. Существуют различные способы управления ИТ-рисками.

Одним из вариантов является минимизация рисков. Компании могут предпринять меры по снижению вероятности наступления угроз или сокращению ущерба. Они могут разделить свой риск со страховыми компаниями или поставщиками, тем самым сократить убытки при наступлении риска, или исключить риск, отказавшись от осуществления бизнес-процессов, которые являются рискованным. Минимизировать риски можно и с помощью оптимизации бизнес-процессов компании.

Другим способом является идентификация уязвимостей. Уязвимости могут не привести к рискам до их эксплуатации, но они должны быть идентифицированы и, если есть возможность, устранены.

Методологической основой проведения ИТ аудита являются международные и внутренние стандарты:[1]

- ГОСТ Р ИСО 19011-2003 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента»;
- IS Standards, Guidelines and Procedures for Auditing and Control Professionals;
- COBIT 4.1 «Control Objectives for Information and related Technology»;
- Федеральное правило (стандарт) аудиторской деятельности №15. «Понимание деятельности аудируемого лица».

Стандарты — источники критериев аудита:

- COBIT 4.1 «Control Objectives for Information and related Technology». Принципы управления. Руководство по аудиту;
- ISO 27001:2005 «Информационные технологии. Методы обеспечения безопасности — Системы управления информационной безопасностью. Требования»;
- ISO 20000 «Управление предоставлением ИТ-услуг»;
- ISO 9000 «Указания по менеджменту качества»;
- Board Briefing on IT Governance.

Данные документы являются ключевыми, но не исчерпывающими, так как этот список при необходимости может быть дополнен.

Польза ИТ аудита и его влияние на деятельность компаний очевидны. Он позволяет оптимизировать расходы на ИТ, снизить затраты, а также сопоставляет затраты, произведенные на ИС и выгоду, которую она приносит для бизнеса.

[1] Основные принципы аудита ИТ. Методы оценки ИТ рисков при проведении аудита [Электронный ресурс]. // IT Expert. – Режим доступа: https://www.itexpert.ru/rus/audit/itaudit/ (дата обращения: 13.01.2019).

В настоящее время информация является важным ресурсом, поэтому нельзя не заметить ее влияние, а также влияние информационных технологий на деятельность предприятий. Но некорректное использование ИТ может привести к возникновению ИТ-рисков. Для того чтобы оценить ИТ и предупредить риски, а затем усовершенствовать используемые ИТ, используют информационный аудит или ИТ-аудит, результатом которого являются разработанные рекомендации для корректировки ИТ системы и ИТ-инфраструктуры компании. Можно управлять рисками, но нельзя полностью их предотвратить. Поэтому после оценки рисков организации необходимо выбрать способ управления ими и правильно его осуществить.

Библиографический список:

1. IT AUDIT: ГЛАВНЫЕ ЦЕЛИ И ОСНОВНЫЕ ЭТАПЫ [Электронный ресурс]. // Простые Технологии. Сервис компьютерных систем. – Режим доступа: http://www.easy-tech.ru/articles/it_audit_glavnye_tseli_i_osnovnye_etapy/

2. Аудит информационных технологий [Электронный ресурс]. // Pba Consult. – Режим доступа: www.pbaconsult.com/ru/services/it-konsalting-i-integratsiya/audit-informatsionnyih-tehnologiy/ (дата обращения: 12.01.2019).

3. Байновский Ф. Информационный аудит [Электронный ресурс] / Ф. Байновский // Риск менеджмент. –2008. – №5-6. – Режим доступа: https://www.cfin.ru/itm/it_audit.shtml (дата обращения: 12.01.2019).

4. Основные принципы аудита ИТ. Методы оценки ИТ рисков при проведении аудита [Электронный ресурс]. // IT Expert. – Режим доступа: https://www.itexpert.ru/rus/audit/itaudit/ (дата обращения: 13.01.2019).

5. Путькина Л. В. Роль информационных систем и технологий в управлении предприятиями сферы услуг [Электронный ресурс] / Л. В.

Путькина // Nauka-rastydent.ru. – 2016. –№ 05 (029). – Режим доступа: http://nauka-rastudent.ru/29/3463/ (дата обращения: 12.01.2019).

6. Стандарты ИТ аудита [Электронный ресурс]. // Help IT.me. Точный сервис. – Режим доступа: https://helpit.me/articles/standarty-it-audita (дата обращения: 13.01.2019).

Оригинальность 90%