*УДК 004.05*

***Руденская Юлия Сергеевна***
***студент магистратуры,***
***1 курс, Институт информационных технологий***
***МИРЭА – Российский технологический университет***
***Россия, г. Москва***
***Потапова Ксения Александровна***
***студент магистратуры,***
***1 курс, Институт информационных технологий***
***МИРЭА – Российский технологический университет***
***Россия, г. Москва***

# МЕТОДИКА ПРОВЕДЕНИЯ ИТ-АУДИТА ОСНОВЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

***Аннотация:*** *изучены основные аспекты проведения аудита информационных технологий на основе риск-ориентированного подхода на основе международных практик и стандартов. Приведены базовые положения стандартов. Рассмотрены показатели эффективности функционирования информационных систем.*

***Ключевые слова:*** *аудит, информационная система, стандарты, риск-ориентированный подход.*

***Abstract:*** *the main aspects of information technology audit based on a risk-based approach based on international practices and standards are studied. The basic provisions of the standards are given. The performance indicators of information systems are considered.*

***Keywords:*** *audit, information system, standards, risk-oriented approach.*

**Введение**

В настоящее время существует необходимость создания методик управления рисками для успешного формирования проектов управленческих решений в информационных системах. Наличие внутреннего аудита позволяет своевременно выявлять проблемы и слабые стороны системы, упрощает процесс принятия долгосрочных управленческих решений, помогает выстраивать грамотную бизнес-логику без мошенничества на различных этапах работы. Грамотность и эффективность принимаемых руководством компании решений напрямую зависит от качества предоставляемой им информации. Такая информация должна быть полной, достоверной, релевантной. Однако часто ответственное лицо вынуждено принимать управленческие решения в условиях риска и неопределенности, которые возникают вследствие передачи ему неактуальной, неполной или ложной информации, что в дальнейшем влечет за собой серьезные последствия. Именно поэтому перед задачей внутреннего аудита ставится цель максимально сократить неблагоприятные риски с помощью их своевременной идентификации и дальнейшей оценки.

Деятельность аудита регламентируется как международными стандартами и положениями, так и локальными документами, которые позволяют выстроить работу внутреннего аудита так, чтобы максимально уменьшить риски от основных бизнес-процессов. При этом, следование сложившимся стандартам и лучшим практикам является необходимым условием для проведения аудита наиболее оптимальным и качественным образом.

**Основные международные стандарты и лучшие практики проведения аудита информационных технологий**

«IT Audit Framework 2nd Edition» (ITAF) – международный стандарт проведения ИТ-аудита от организации ISACA, действующая редакция выпущена в июле 2013 года. Стандарт используется при проведении аудиторских проверок информационных систем и ИТ-инфраструктуры. Стандарт определяет основные термины и концепции, требования к специалистам, этапы проведения проверок

и подготовки отчетов, перечень руководств, рабочих программ и инструментальных средств, используемых в области ИТ-аудита.

ITAF состоит из трех частей:

– общие стандарты;

– стандарты проведения аудиторских проверок;

– стандарты отчетности.

Для каждой из частей стандарта ассоциацией ISACA разработаны руководства, рабочие программы и инструкции, поддерживающие проведение описанных аудиторских процедур [3].

«Cobit 5 for Assurance» – руководство по проведению аудита в соответствии с COBIT v.5, действующая редакция выпущена в июле 2013 года. Руководство предназначено для использования специалистами в области ИТ-аудита, ИТ-рисков и управления ИТ при проведении аудиторских проверок информационных систем в соответствии со сборником лучших практик COBIT 5.

«Cobit 5 for Assurance» включает в себя:

– содержит детальное руководство по использованию COBIT 5 для организации и поддержания функции внутреннего ИТ-аудита в компаниях;

– содержит структурированный подход к проведению ИТ-аудита в соответствии с процессами и факторами, описанными в COBIT 5;

– демонстрирует конкретные примеры использования «COBIT 5» при проведении ИТ-аудита.

В сравнении с ITAF, руководство «Cobit 5 for Assurance» обладает меньшей степенью формализации аудиторских процедур и более широким покрытием вопросов организации ИТ-процессов в соответствии с лучшими практиками.

«International Professional Practices Framework (IPPF) for Internal Auditing Standards» – международный стандарт проведения внутреннего аудита от Института Внутренних Аудиторов (IIA). Действующая редакция выпущена в 2013 году. Целевая аудитория стандарта – сотрудники внутреннего аудита. Стандарт направлен на определение базовых принципов проведения

внутреннего аудита, стандартного набора практик проведения внутреннего аудита, базовых показателей оценки эффективности процедур внутреннего аудита. Стандарт может быть использован как при проведении внутреннего финансового и операционного аудита, так и при проведении внутреннего аудита информационных технологий. Для методологической поддержки стандарта в части проведения ИТ-аудита, ассоциацией IIA были разработаны детальные руководства по оценке ИТ-рисков (Guide to the Assessment of IT Risk) и аудиту информационных технологий (Global Technology Audit Guide) [3].

В некоторых случаях при проведении ИТ-аудитов могут быть использованы международные стандарты и лучшие практики, которые не являются непосредственными стандартами аудита, но удобны для оценки эффективности ИТ-процессов:

– ISO 20000 – международный стандарт по управлению и обслуживанию IT сервисов;

– ITIL (IT Infrastructure Library) – библиотека, описывающая лучшие методы организации работы подразделений или компаний, предоставляющих услуги в области ИТ;

– PCI DSS – стандарт безопасности данных индустрии платёжных карт, учреждённый международными платёжными системами Visa, MasterCard, American Express, JCB и Discover;

– Публикации NIST серии 800-xx по информационной безопасности;

– ISF Standards of Good Practice for Information Security – бизнес-ориентированное практическое руководство по управлению рисками информационной безопасности от международной организации Information Security Forum (ISF) [3].

Аудит информационных систем является важнейшей составляющей аудита компании в целом. Информационная система (ИС) представляет собой совокупность программного и аппаратного обеспечения, используемого для обработки, передачи, изменения и хранения информации, подразумевая в своем составе широкий набор элементов. ИС в более узком смысле представляет собой

конкретный программный продукт. Основная задача при проведении аудита в компьютерной среде обработки данных является решение вопроса о достоверности предоставляемой информации. Главная цель методологии аудита ИС – достижение высокого уровня уверенности в эффективности функционирования ИС в следующих показателях:

– принципы функционирования (совместимость, адаптивность, гибкость);

– методы функционирования (соответствие нормативной и технической документации);

– способы функционирования (фактические показатели функционирования) [2].

Таким образом, деятельность аудита становится направленной на риск-ориентированный подход, который дает своевременную оценку эффективности работы информационной системы, выявляет негативные и положительные аспекты работы, формирует рекомендации для дальнейшего развития. Один из способов внутреннего аудита – система мониторинга, включающая обработку информации для оценки рисков и прогнозирования, проекты по принятию решений и повышению эффективности компании в целом.

Потенциал внутреннего аудита в современных условиях заключается в создании системы мониторинга для управления ключевыми бизнес-процессами. Основой такой системы мониторинга является формирование проектов управленческих решений и применение процедур, направленных на повышение эффективности деятельности компании, а также получения информации, необходимой для оценки рисков и прогнозировании развития общества. Именно поэтому внутренний аудит в случае системного подхода к решению основных проблем приобретает приоритетное значение в системе корпоративного управления и формирует необходимые предпосылки для развития профессии внутреннего аудитора. Согласно мнению специалистов, внутренний аудит можно рассматривать по-разному: как подсистему внутреннего контроля; как составную часть независимого аудита; как элемент системы риск-менеджмента.

Внутренний аудит, основанный на риск-ориентированном подходе, должен базироваться на эффективных методиках и процедурах, использование которых позволит своевременно выявить риски и факторы неэффективной работы системы.

**Использованные источники:**

1. Шарапова И.С., Юга И.П., Кваско М.А. Концепция риск-ориентированного аудита // Молодой ученый. – 2017. – №10. – С. 292-296. – Режим доступа. – URL: https://moluch.ru/archive/144/40397/ (дата обращения: 18.01.2020).

2. Баранова О.В. Методологические подходы к аудиту информационных систем [Текст] / Баранова О.В. // Аудит и финансовый анализ. – 2015.

3. Основные международные стандарты и лучшие практики проведения аудита информационных технологий // [Электронный ресурс] – Режим доступа. – Url: https://habr.com/ru/post/224895/ (дата обращения: 18.01.2020).

4. Толчинская М.Н. Риск-ориентированный подход в организации службы внутреннего аудита / М.Н. Толчинская // Фундаментальные исследования. – 2015. – № 10. – С. 640–644.