

## ИТ-АУДИТ. РИСКИ В ИТ-АУДИТЕ

## IT-AUDIT. RISKS IN IT-AUDIT

**Заиграев Евгений Алексеевич**, студент ФГБОУ ВО «Сибирский государственный университет путей сообщения», г. Новосибирск, Россия

**Зайцева Татьяна Сергеевна**, старший преподаватель ФГБОУ ВО «Сибирский государственный университет путей сообщения», г. Новосибирск, Россия

**Zaigraev Evgeniy Alekseyevich**, student, Siberian Transport University, Novosibirsk, Russia

**Zaitseva Tatyana Sergeyevna**, senior lecturer, Siberian Transport University, Novosibirsk, Russia

**Аннотация.** В современном мире руководство компании часто сталкивается с проблемой улучшения работы предприятия. Для это необходимо проверять деятельность своих сотрудников как отдельно, так и работу организации полностью. В данной статье описываются основные цели ИТ-аудита для предприятия или бизнеса в целом. Также рассказывается об основных видах аудиторской проверки. Так как аудиторские проверки имеют последствия, как хорошие, так и плохие, будет затронута тема рисков и их описание.

**Abstract.** In modern world companies' heads often face problems on improvement of work in ventures. For this aim it is necessary to examine the activity of the company's workers separately as well as the work of the whole company. The paper depicts main goals of IT-audit for a venture and business in general. There are also given principal types of audit check in the paper. As it results in not only good but bad consequences, there are also discussed the problem of risks and their description.

**Ключевые слова:** ИТ-аудит, информационные технологии, оценка, диагностика, риски, проверка.

**Key words:** IT audit, information technology, assessment, diagnostics, risks, verification.

Многие компании и руководители сталкивались с проблемами проведения ИТ-аудита. В определенный период времени или под конец года возникает такая потребность, как проверка действий своих сотрудников или полностью своей компании на правильность действий и соответствие компетенций. Для это и необходим ИТ-аудит.

По легальному определению ИТ-аудит – это оценка и диагностика состояния информационных технологий и процессов в компании, насколько они отвечают требованиям конкретного предприятия и бизнеса.

Можно выделить семь основных целей ИТ-аудита предприятия:

1. Оценка эффективности расходуемого бюджета. Данная цель включает в себя анализ затрат на заработные платы специалистов, капитальные затраты на оборудование, а также переменные затраты;

2. Оценка эффективности работы ИТ-отдела, а также проверка уровня подготовки кадров.

3. Оценка места в инфраструктуре и бизнес-процессах, где информационные системы используются не так эффективно, как могли бы. Также вырабатываются рекомендации по повышению эффективности и перераспределение нагрузки.

4. Оценка работы процессов и систем, обеспечивающие информационную безопасность компании.

5. Оценка рисков информационных активов компании, а также определение методов минимизации этих рисков.

6. Обеспечение соответствия информационной системы с законами и стандартами отрасли предприятия.

7. Разработка дорожной карты для дальнейшего устранения проблем.

В данной статье хочется выделить четыре вида IT-аудита, первый из которых называется экспресс-обследование. В процессе данного обследования готовятся и структурируются общие данные о текущем состоянии информационной инфраструктуры.

Результатом данной проверки является отчет, в котором прописывается общее описание IT-инфраструктуры как она есть на этот период времени. Чаще всего это формируется с поверхностным анализом и набором минимальных рекомендаций.

Следующий вид – аудит бизнес-процесса. Здесь проводится анализ IT-инфраструктуры не для компании или предприятия в целом, а только для определенного бизнес-процесса. Например, аудит компьютерной техники, программного обеспечения, персонала, задействованного в данном бизнес-процессе либо аудит самого процесса. Результатом является отчет о состоянии процесса в настоящем времени, рекомендации об улучшении отдельных элементов IT-структуры, оценка рисков.

Третий вид IT-аудита – аудит по критерию. Данная проверка подразумевает в себе сбор и анализ сведений об информационных системах, но только в разрезе какого-либо выбранного критерия. Такими критериями могут быть: быстродействие, безопасность, надежность, производительность и другие. В конце проверки также формируется отчет с оценкой соответствия или несоответствия работы IT-системы выбранному критерию.

Комплексный IT-аудит – четвертый вид проверки. Общие действия аудита предполагают, что работа информационной инфраструктуры будет изучена и оценена максимально подробно. Результатом данного аудита является отчет с соответствиями потребностей бизнеса в целом, и как происходит стратегическое развитие и совпадает ли оно с планами развития бизнеса.

Одной из главных проблем любой аудиторской проверки является теория рисков и внутреннего контроля. Под определением аудиторского риска подразумевается риск выражения неправильного мнения в случаях, когда в отчетах содержатся значительные искажения. Можно выделить четыре вида риска в аудиторской проверке:

1. Риск существенного искажения (Risk of material misstatement). Данный вид риска подразумевает неустойчивое положение в финансовой отчетности, выявляемое на стадиях, предшествующих внешнему аудиту.

2. Неотъемлемый риск (IR – Inherent risk). В данной ситуации рассматривается риск дебетовых и кредитных оборотов по счетам бухгалтерского учета за проверяемый период, а также конкретные статьи бухгалтерского баланса на отчетную дату с искажениями.

3. Риск системы контроля (CR – Control risk). При эффективности системы выделяют контрольную среду, информационную среду, а также мониторинг средств контроля и процесс оценки рисков предприятия или бизнеса.

4. Риск необнаружения (DR – Detection risk) – риск, предусматривающий то, что процедуры аудиторской проверки направлены на снижение аудиторского риска до низкого уровня. Это не дает возможности обнаружить существенные искажения, которые, по сравнению с другими, могут быть значительными в совокупности или по отдельности с другими искажениями.

Все представленные виды аудита имеют связь между собой. Чтобы избежать значительных рисков, необходимо осуществлять контроль за деятельностью компании в целом и проводить внутренний аудит как можно чаще. Это поможет руководителю и менеджерам каждого подразделения не допускать существенных искажений и быть готовым к аудиторским проверкам высшего ранга.

### **Библиографический список**

1. Бурцев В.В. Организация системы внутреннего контроля коммерческой организации / В.В. Бурцев. — М.: Экзамен, 2015. — 320 с.

2. Бизнес-план для привлечения финансирования: официальный сайт URL: [https://www.cfin.ru/finanalysis/risk/material\\_misstatement.shtml](https://www.cfin.ru/finanalysis/risk/material_misstatement.shtml)(дата обращения 27.04.2020)

3. Суйц В.П. Внутрипроизводственный контроль / В.П. Суйц. – М.: Финансы и статистика, 2016. — 127 с.

### **Bibliography**

1. Burcev V.V. Organizacija sistemy vnutrennego kontrolja kommercheskoj organizacii / V.V. Burcev. — M.: Jekzamen, 2015. — 320 s.

2. Biznes-plan dlja privlechenija finansirovanija: oficial'nyj sajt URL: [https://www.cfin.ru/finanalysis/risk/material\\_misstatement.shtml](https://www.cfin.ru/finanalysis/risk/material_misstatement.shtml) (data obrashhenija 27.04.2020)

3. Sujc V.P. Vnutriproizvodstvennyj kontrol' / V.P. Sujc. – M.: Finansy i statistika, 2016. - 127 s.

### **Сведения об авторах**

1. Заиграев Евгений Алексеевич, студент ФГБОУ ВО «Сибирский государственный университет путей сообщения», [zheka25201305@gmail.com](mailto:zheka25201305@gmail.com)

2. Зайцева Татьяна Сергеевна, старший преподаватель ФГБОУ ВО «Сибирский государственный университет путей сообщения»

### **Authors' personal details**

1. Zaigrayev Evgeniy Alekseyevich, student, FSBEI HE Siberian Transport University, [zheka25201305@gmail.com](mailto:zheka25201305@gmail.com)

2. Zaitseva Tatyana Sergejevna, senior lecturer, FSBEI HE Siberian Transport University

© Заиграев Е.А., Зайцева Т.С., 2020.