УДК 004.05

МЕТОДИКА ПРОВЕДЕНИЯ ИТ-АУДИТА НА ОСНОВЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

Руденская Ю.С., Андрианова Е.Г.

МИРЭА – Российский технологический университет, 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: rudenskaya96@yandex.ru, andrianova@mirea.ru

В настоящее время проблема совершенствования и развития ИТ-аудита связана с необходимостью повышения его качества с целью увеличения надежности, безопасности и отказоустойчивости информационных систем. В данной статье рассмотрены основные аспекты проведения технического аудита информационных технологий на основе риск-ориентированного подхода.

Ключевые слова: ИТ-аудит, методика, риск-ориентированный подход, информационная система, бизнес-процесс.

METHODOLOGY FOR CONDUCTING AN IT-AUDIT BASED ON A RISK-BASED APPROACH

Rudenskaya Y.S., Andrianova E.G.

MIREA - Russian Technological University, 119454, Russia, Moscow, Vernadscogo avenue, 78, e-mail: rudenskaya96@yandex.ru, andrianova@mirea.ru

Currently, the problem of improvement and development IT-audit is associated with the need to improve its quality in order to increase the reliability, security and resiliency of information systems. This article discusses the main aspects of conducting a technical audit of information technologies based on a risk-based approach.

Key words: IT audit, methodology, risk-based approach, information system, business-process.

Введение

Использование современных информационных систем и технологий в деятельности предприятия приводит к появлению рисков, не характерных при обработке данных вне компьютерной среды.

В последние годы большое внимание уделяется ИТ-аудиту инфраструктуры предприятия. Под этим термином подразумевается комплекс мероприятий, направленный на получение и оценку объективных данных о состоянии информационных технологий: соответствия потребностям бизнеса, современной конъюнктуре, технологиям, подходам к работе.

Информационная инфраструктура предприятия представляет собой комплекс элементов, обеспечивающих функционирование и развитие информационного пространства, а также средства информационного взаимодействия. ИТ-инфраструктура включает в себя не только совокупность аппаратного и программного обеспечения, но и средства обеспечения доступа пользователей к информационным ресурсам.

Методика ИТ-аудита рассматривается преимущественно в технических аспектах функционирования, оказывающих влияние на обеспечение непрерывности работы, поддержание заданных значений показателей надежности, сокращение эксплуатационных расходов и численности персонала, возможность управления качеством услуг дистанционного обслуживания, а также составление отчетности предприятия.

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.

Риск-ориентированный подход к ИТ-аудиту

Риск – это вероятность наступления действия или события, которое может оказать неблагоприятное воздействие на организацию или информационные ресурсы.

Риск-ориентированный подход при проведении аудита дает своевременную оценку эффективности

работы информационной системы, выявляет негативные и положительные аспекты работы, формирует рекомендации для дальнейшего развития.

Риск-ориентированный подход заключается в том, что учитывает следующие типы рисков:

– неотъемлемый риск: возможность наличия существенных ошибок в отчетности, при допущении отсутствия соответствующих внутренних средств контроля;

– риск контроля: вероятность того, что ошибка, которая может произойти в области аудита, не будет предотвращена, обнаружена и своевременно исправлена системой внутреннего контроля;

– риск обнаружения: возможность того, что процедуры проверки не обнаружат нарушения, которые могут быть существенными по отдельности или в сочетании с другими ошибками.

Все больше и больше организаций переходят к подходу проведения аудита, основанному на оценке рисков, который можно адаптировать для развития и улучшения процесса непрерывного внутреннего аудита.

Этапы методики проведения ИТ-аудита на основе риск-ориентированного подхода

Рассмотрим методику проведения ИТ-аудита на основе риск-ориентированного подхода.

Этап 1. Планирование аудита.

На этом этапе проводится анализ ИТ-инфраструктуры предприятия с целью определения зоны проведения аудита, соблюдения законов и профессиональных стандартов. Совместно с представителями предприятия формируется Регламент аудита, в котором отражается следующее:

– цели и задачи проведения аудита ИТ-инфраструктуры, ключевые показатели работы систем;

– полномочия аудиторов в отношении выполняемой работы по оценке рисков, право на доступ к внутренней информации;

– сроки и порядок формирования отчетности о результатах.

Этап 2. Оценка рисков и анализ бизнес-процессов.

Подход к аудиту информационных систем, основанный на оценке риска, позволит разработать общий и эффективный план аудита, который будет учитывать все потенциальные недостатки и/или отсутствие средств контроля и определять, может ли это привести к значительным потерям или уязвимостям.

На данном этапе выполняются следующие шаги (рис. 1):

– определение бизнес-процессов, в которых риск неприемлемо высок;

– определение систем контроля, направленных на устранение высоких рисков;

– оценка неопределенности, которая существует в отношении критических систем управления.

Рисунок 1. Анализ бизнес-процессов и проверка средств контроля

Для каждого протекающего бизнес-процесса необходимо определить список угроз, которые могут произойти. Таким образом, будет складываться представление о бизнес-процессах предприятия, формироваться схема внутреннего контроля и выявляться его слабые места.

Этап 3. Выполнение аудиторской работы.

Основываясь на ранее полученной оценке рисков и выявленных слабых областях, необходимо приступить к разработке Плана аудита и Программы аудита. План аудита детализирует характер, цели, сроки и объем ресурсов, необходимых для аудита. Программа аудита подробно описывает характер, сроки и объем аудиторских процедур.

В Плане аудита могут быть выполнены различные контрольные тесты и проверки (рис. 2).

Проверки должны охватывать следующие области:

– структура информационных ресурсов;

– приобретение новых систем и расширение существующих;
– закупка и поддержка оборудования, программного и аппаратного обеспечения;
– мониторинг процессов окружающей среды;
– уровень конфиденциальности, целостности, доступности, информации, хранящейся в ИС;
– уровень использования доступных ИТ-ресурсов, включая прикладные программы и приложения.

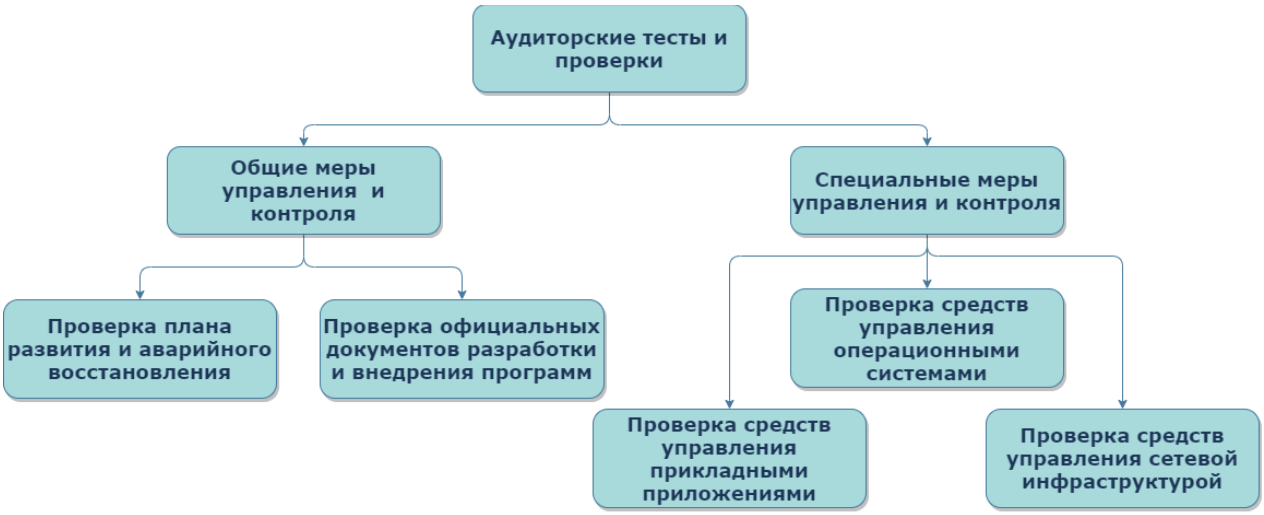

Рисунок 2. Обзор аудиторских проверок

Компьютерные методы проверки являются важными инструментами для аудитора и представляют собой анализ тестовых данных, системы мониторинга и отслеживания, а также экспертные системы аудита.

Этап 4. Отчётность

После выполнения всех соответствующих проверок аудитор составляет отчёт, сообщающий о результатах аудита. Отчёт содержит в себе информацию об исследуемом предприятии, период проверок и объем аудиторской работы, выводы и ограничения, аудиторские доказательства.

Регулярный аудит ИТ-инфраструктуры помогает оценить ее актуальное состояние, выявить слабые места и недостатки, получить практические рекомендации касательно того, какие изменения следует внести для повышения эффективности системы и снижения затрат. Кроме того, аналитические работы помогут рационализировать и сократить расходы на ИТ-сферу, оценить информационные риски и повысить уровень управляемости предприятием.

Заключение

ИТ-аудит является практически незаменимым инструментарием при разностороннем исследовании и оценке информационной инфраструктуры, принятии управленческих решений, прогнозировании развития всей бизнес-системы и ее информационной системы, а также инструментом поддержки управления этими системами. Одно из необходимых средств при проведении аудита – это системы мониторинга, например, Zabbix и Nagios, включающие обработку информации для оценки рисков и прогнозирования, проекты по принятию решений и повышению эффективности компании в целом.

Список литературы

1. Алборов Р. А. Аудит в организациях промышленности, торговли и АПК / Р.А. Алборов. - М.: Дело и сервис, 2019. - 432 с.

2. Василенко А. А. Стандарты аудита. Изучайте и внедряйте / А.А. Василенко, О.В. Овчаренко. - М.: Феникс, 2019. - 410 с.

3. Камышанов П.И. Практическое пособие по аудиту / П.И. Камышанов. - М.: ИНФРА-М, 2019. - 522 с

4. Основные международные стандарты и лучшие практики проведения аудита информационных технологий // [Электронный ресурс] – Режим доступа. – Url: https://habr.com/ru/post/224895/ (дата обращения: 01.02.2021).

5. Суворова С.П. Международные стандарты аудита / С.П. Суворова, Н.В. Парушина, Е.В. Галкина. - М.: Инфра-М, Форум, 2019. - 320 с.

6. Юдаев И.А., Андрианова Е.Г. Направления совершенствования аудита информационных систем ИТ-Стандарт. 2018. № 4 (17). С. 67-73.

References

1. Alborov R.A. Audit in organizations of industry, trade and agriculture / R.A. Alborov. - M.: Delo i service, 2019. - 432 p.

2. Vasilenko A. A. Audit standards. Study and implement / A. A. Vasilenko, O. V. Ovcharenko. - M.: Phoenix, 2019. - 410 p.

3. Kamyshanov P.I. Practical guide to audit / P.I. Kamyshanov. - M.: INFRA-M, 2019. - 522 p.

4. Basic international standards and best practices of information technology audit // [Electronic resource] - Access mode. - url: https://habr.com/ru/post/224895/ (accessed: 01.02.2021).

5. Suvorova S.P. International standards of audit / S.P. Suvorova, N.V. Parushina, E.V. Galkina. - M.: Infra-M, Forum, 2019. - 320 p.

6. YUdaev I.A., Andrianova E.G. Napravleniya sovershenstvovaniya audita informacionnyh sistem IT-Standart. 2018. № 4 (17). S. 67-73.