УДК 657.6:004(045)

АУДИТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В.В. Иванченко

Аннотация. В работе рассмотрены различные виды ИТ-аудита; кратко перечислены стандарты, используемые при проведении ИТ-аудита; описан подход к проведению аудита и польза от его проведения.

Ключевые слова: ИТ-аудит, стандарты ИТ-аудита, подход к проведению ИТ-аудита.

Abstract. In this article different types of IT audit are described, the standards of IT audit are briefly listed, IT audit approach and the benefits of its holding are given.

Keywords: IT audit, IT audit standards, IT audit approach.

Информационные технологии постоянно совершенствуются и усложняются. Положительные аспекты от использования информационных технологий в бизнесе затеняются новыми рисками. Например, столь популярная сегодня электронная коммерция связана с обработкой конфиденциальной информации различного рода: финансовые транзакции, персональные данные, сведения о торгах [1].

Это, в свою очередь, требует дополнительного контроля со стороны высшего менеджмента, внешнего и внутреннего аудита. Именно поэтому аудит информационных технологий проводят в компаниях для того, чтобы оперативно получать систематизированную и достоверную информацию для оценки состояния ИТ, принятия решений по управлению ИТ.

Безусловно, аудит бывает разный. Аудит можно классифицировать по различным признакам, но здесь мы будем говорить только об ИТ-аудите – проверка функционирования и защиты информационных систем.

В первую очередь необходимо сформировать общее понимание того, что такое ИТ-аудит и для чего он нужен. Под термином «аудит ИТ» понимается процесс получения систематизированных и объективных данных о текущем состоянии ИТ и оценки степени их соответствия «лучшим практикам» [2].

Целью ИТ-аудита является совершенствование системы контроля за ИТ. Для этого аудиторы как внешние, так и внутренние должны:

- осуществлять оценку рисков ИТ;
- содействовать предотвращению и смягчению сбоев ИС;
- участвовать в управлении рисками ИТ;
- помогать подготавливать нормативные документы;
- помогать связать бизнес-риски и средства автоматизированного контроля;
- осуществлять проведение периодических проверок;
- содействовать ИТ-менеджерам в правильной организации управления ИТ;
- осуществлять «взгляд со стороны».

В России, как и за рубежом, представлено шесть видов услуг по аудиту информационных технологий [3]:

- Обследование ИТ.
- Экспертная оценка ИТ.
- Технический аудит ИТ.
- Аудит ИТ бизнес-процесса.
- Аудит критерия ИТ.
- Комплексный аудит ИТ.

Обследование ИТ – сбор информации, которая будет использоваться для проведения дальнейших работ, например, работ, связанных с внедрением новой информационной системы или оптимизации и модернизации уже существующей. В этом случае данный вид аудита используется с целью грамотно собрать достоверную информацию о текущем состоянии ИТ. Стоит отметить, что в данном случае речь об анализе и оценке собранной информации не идет.

Экспертная оценка ИТ – это оценка адекватности финансирования проектных решений и/или инвестиций в закупку оборудования и ИТ-услуг. При этом возможны следующие виды оценок:

- оценка ИТ-проектов или проектных решений;
- оценка обоснованности инвестиций в ИТ;
- оценка стоимости ИТ-составляющей компании;
- оценка текущих ИТ-проектов;
- оценка возможности перепрофилирования ИТ-инфраструктуры;
- оценка организации эксплуатации ИТ;
- оценка подготовки пользователей.

Технический аудит ИТ – это сбор, анализ информации с последующим формированием и выдачей рекомендаций по оптимизации работы конкретного технического элемента ИТ-инфраструктуры. Как правило, данный вид аудита имеет малый масштаб работы и направлен на узкую техническую специализацию исследования.

Аудит ИТ бизнес-процесса – это аудит информационных технологий и систем, критичных для выполнения конкретного бизнес-процесса компании с заданными критериями качества и эффективности. Одним из важнейших результатов этого вида аудита является формализованная модель исследуемого бизнес-процесса.

При проведении аудита ИТ бизнес-процесса, как правило, выполняется:

- определение ответственного за процесс;
- определение пользователей и участников бизнес-процесса;
- выявление применяемого оборудования и программ;
- оценка действий обслуживающего персонала и пользователей;
- анализ проектных и регламентирующих документов.

Аудит критерия ИТ – это сбор, анализ информации и выдача рекомендаций по какому-то выбранному критерию ИТ, например, безопасность, производительность, надежность, доступность и т.д. При проведении аудита по определенному критерию оценки принято исследовать не только отдельный элемент ИТ-инфраструктуры, но и всю совокупность программных, аппаратных средств, процессов их сопровождения и обслуживания во всей проверяемой компании.

Комплексный аудит ИТ – это аудит, при котором осуществляется определение и анализ взаимосвязей бизнес-процессов, их требований, информационных и смежных технологий, совокупности программно-аппаратных средств с целью сравнения адекватности ИТ потребностям бизнеса компании.

Если говорить о ИТ-аудите в рамках финансового аудита, то он содержит в себе некоторые части от вышеперечисленных видов. Таким образом, он представляет собой некоторый обобщенный вид без детального углубления в те или иные области. Своеобразная «поверхностность» аудита в данном случае обусловлена спецификой и конечной целью – подтверждение финансовой отчетности, а не детальная проверка информационных систем предприятия и его систем безопасности, а также процессов управления этими системами.

В настоящее время существует множество стандартов, регламентов, лучших мировых практик, которые используются аудиторами в ходе проверки функционирования информационных систем.

На рис. 1 представлен перечень стандартов информационной безопасности, разделенный на 3 группы:

- международные стандарты;
- государственные (национальные) стандарты РФ;
- руководящие документы.

Также аудиторские команды довольно часто используют и другие стандарты, такие, как Cobit, ITIL, TOGAF, PMBOK, CMM и другие.

Концепция аудита информационных систем исходит из суждения о том, что основным объектом выступает информационная система [4].

На сегодняшний день существует большое количество определений понятия «информационная система». Вот лишь некоторые из них:

- информационная система – это совокупность, состоящая из одного либо нескольких компьютеров, соответствующих средств программирования, операторов, физических процессов, средств телекоммуникаций и других, образующих автономное целое, способное осуществлять обработку или передачу данных [5];
- информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [6];
- информационная система – это совокупность программных и аппаратных средств, а также организационное обеспечение, которые все вместе оказывают информационную поддержку человеку в различных сферах его деятельности [7].

Насколько бы велико не было разнообразие определений, авторы сходятся в одном мнении, что информационная система – это, в первую очередь, совокупность информации и программных и технических средств, используемых для ее обработки, хранения и передачи.

При оценке эффективности принципов функционирования информационной системы разумная степень уверенности достигается в отношении нерушимости и полной гармонизации элементов информационной системы, адаптивности информационной системы к воздействиям внешней среды, а также в отношении совместимости информационной системы для обработки финансовой информации с другими информационными системами. При оценке эффективности методов функционирования информационной системы разумная сте-

пень уверенности достигается в отношении административных решений в части обязательного исполнения законов, директив, приказов и аналогичных регламентов, направленных на использование информационной системы в бизнес-процессах экономического субъекта, а также в отношении экономических и социально-идеологических решений в части материальной и социальной мотивации сотрудников, направленной на эксплуатацию и улучшение действующих характеристик информационной системы. При оценке эффективности способов функционирования информационной системы разумная степень уверенности достигается в отношении соответствия описательной модели, содержащейся в технической документации, фактическим показателям ее функционирования, а также в отношении эффективности работы аппаратного обеспечения.

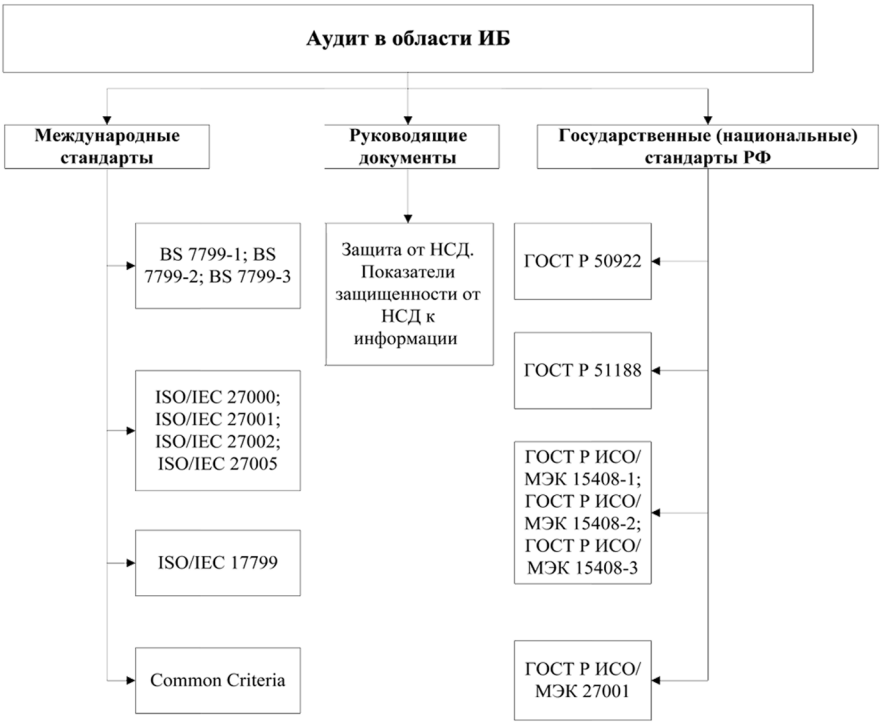

Рис. 1. Стандарты аудита в области информационной безопасности

Средства контроля в системах, использующих ИТ, состоят из сочетания средств ручного и автоматизированного контроля (например, средства контроля, встроенные в компьютерные программы). Ручной контроль может не зависеть от ИТ, в нем может использоваться информация, составленная с помощью ИТ, или он может быть ограничен мониторингом эффективного функционирования ИТ или автоматизированным контролем. Одновременное использование организацией ручного и автоматизированного контроля зависит от характера и сложности использования организацией ИТ.

Согласно «Стандартам аудиторской деятельности»: «Общие средства контроля в информационных системах (ОСКИС) представляют собой политики и процедуры, которые имеют широкие области применения и предназначены для обеспечения эффективного функционирования прикладных средств контроля, помогая удостовериться в правильном бесперебойном функционировании информационных систем» [8]. Тестирование общих средств контроля может дать поверхностную картину функционирования информационной системы, а также вполне достаточное основание для принятия решения о дальнейшем продолжении проведения ИТ-аудита. Если на уровне ОСКИС выявлены серьезные недостатки, то дальнейшее тестирование может быть бессмысленно.

При понимании уровня тестирования общих средств контроля в информационных системах необходимо достичь понимания соответствующего контроля, зависимого от ИТ, применимого к соответствующим приложениям, файлам с данными и компонентам технологии.

Также целесообразно понять подход организации к управлению информационными технологиями. Например, необходимо понять, как организованы центры хранения данных (datacenter), как и где осуществляется управление и контроль процессов внесения изменений в программы, архитектура безопасности организации и подход к безопасности, использование сторонних сервисных организаций или общекорпоративных служб и т.п.

Таким образом, после сбора необходимой информации аудитор может сделать вывод об эффективности функционирования ИС.

Из всего вышеперечисленного можно сделать вывод о том, что аудит информационных систем – это достаточно сложный процесс, требующий от аудитора хорошей технической подготовки, четкого по-

нимания того, что он должен сделать и для чего это делается. Также необходимо учитывать специфику отрасли компании, в которой проводится ИТ-аудит, так как для компаний, например, телекоммуникационной и нефтедобывающей отраслей подход к проведению аудита может различаться.

Для чего же так необходим ИТ-аудит в современном мире? В первую очередь, результаты могут быть полезны для руководства компании. Основываясь на результатах ИТ-аудита, можно понять, правильно ли функционирует построенная ИТ-инфраструктура и какое влияние она оказывает на развитие бизнеса. С другой стороны, в положительных результатах такого аудита может быть заинтересован ИТ-департамент, так как от этого может зависеть дальнейшее развитие отдела и его сотрудников в рамках компании: чем лучше результаты, тем с большей охотой руководство компании будет инвестировать в ИТ.

ИТ-аудит позволяет оценить соответствие информационных систем требованиям бизнеса и различным стандартам, призванным повысить эффективность ИТ, а также построить долгосрочную стратегию развития информационных технологий. В результате ИТ-аудита может быть получена оценка себестоимости ИТ-услуг, на основании которой в дальнейшем можно принять решение о выводе некоторых функций на аутсорсинг или же концентрации всех функций внутри фирмы, а также выявить потенциальные риски и «узкие» места в ИТ-инфраструктуре, чтобы разработать соответствующие процедуры по их минимизации.

ЛИТЕРАТУРА

1. *Ерохин С.С.* Методика аудита информационной безопасности. – Томск, 2010.

2. *Киль М.* Аудит информационных технологий как средство корпоративного управления. Презентация.

3. Аудит информационных технологий компанией РВА. [Электронный ресурс]. URL: http://pbaconsult.com/index.php?page=53&lang=ru.

4. *Маслова И.А., Ветрова А.А.* Основные направления оптимизации рисков при проведении аудита информационных систем // Управленческий учет. 2014. №1.

5. Внутренняя библиотека Дальневосточного университета путей и сообщения, лекция по информационным системам. [Электронный ре-

сурс]. URL: http://edu.dvgups.ru/METDOC/ITS/STRPRO/INF_TEH_STR/METOD/SULDIN/frame/5.htm

6. Федеральный закон РФ от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. URL: http://www.rg.ru/2006/07/29/informacia-dok.html

7. Определение и классификация информационных систем, IT CONCORD. [Электронный ресурс]. URL: http://itconcord.ru/articles/information-system

8. Стандарты аудиторской деятельности. – М, 2012.

В.В. Иванченко,
студент, Финансовый университет при Правительстве РФ
E-mail: leraivanchenko@yahoo.com