

Автоматизация аудита информационной системы предприятия энергетической отрасли

Понятие аудита информационной системы (ИС) предприятия оформилось сравнительно недавно и сегодня вызывает постоянный интерес специалистов в области информационных технологий и менеджмента. Статья раскрывает принципы логического проектирования системы автоматизации аудита ИС в энергетической отрасли.

Аудит ИС предприятия энергетической отрасли представляет собой комплексный контроль выполнения функций поддержки основных бизнес-процессов, реализующихся на предприятии с учетом проблемной области ИС. В нашем случае проблемной областью является энергетическая отрасль. Основные бизнес-процессы на предприятиях отрасли:

- закупка топлива;
- выработка, учет, отпуск тепловой и электроэнергии;
- транспортировка тепловой и электроэнергии;
- продажа тепловой и электроэнергии.

Обычно на ИС предприятия возлагается задача обработки информации, связанной с движением материальных и финансовых средств.

Ошибки, допущенные при проектировании ИС, а также последствия нарушений системы защиты информации сопряжены со значительными финансовыми потерями. Все это обуславливает необходимость автоматизации аудита ИС и делает актуальной задачу логического проектирования системы автоматизации аудита ИС в энергетической отрасли.

Методология аудита информационной системы

Аудит информационной системы предприятия энергетической отрасли основывается на следующих стандартах и нормах:

- ISA (International Standards on Auditing) — международные аудиторские стандарты;

- международный стандарт ISO/IEC 17799:2000 «Управление информационной безопасностью — Информационные технологии (Information Technology — Information Security Management)»;

- стандарт CobiT (The Control Objectives for Information and Related Technology — Контрольные объекты для информационной и смежных технологий);

- стандарты Ассоциации аудита и управления информационными системами (The Information Systems Audit and Control Association & Foundation Standards — ISACA Standards), составленные на основе CobiT [2];

- ГОСТ 15 408 — «Критерии оценки безопасности информационных технологий», который рассматривает частный вопрос аудита, раскрываемый CobiT;

- опыт аудита в энергетике.

Учитывая, что аудит ИС так или иначе основывается на международных стандартах, рассмотрим содержание основных из перечисленных нормативных документов.

Международные стандарты ISO

Для проведения аудита информационной системы компании-аудиторы в основном опираются на международный стандарт ISO/IEC 17799:2000 «Управление информационной безопасностью — Информационные технологии (Information technology — Information Security Management)», а также на стандарт ISO 15 408–99 «Общие критерии». Эти стандарты охватывают следующий круг вопросов [3]: