Аннотация

Тема дипломного проекта «Управление безопасностью организации с применением системы Open Source Security Information Management». Проект внедрялся в компанию «Просто Бэк-Офис». В данной работе была проанализирована архитектура SIEM системы, исследованы и сравнены различные SIEM системы, выбрана система OSSIM и на её основе спроектирована система сбора и корреляции событий информационной безопасности. Показаны сравнение OSSIM с платной версией системы USM, разработана структурная схема корпоративной сети после введения системы , также была произведена атака «BruteForce» на устройство в сети и были показаны результаты выявления системой. Также были рассмотрены инструменты системы, такие как хостовая система обнаружения вторжений - OSSEC, сетевая система обнаружения вторжений - Suricata, сканер активов - Nagios, сканер уязвимостей - OpenVAS.

Проведен анализ условий труда с расчетом системы кондиционирования и пожарной безопасности.

Были рассчитаны риски информационной безопасности, задачей которых являлось понимание реальных угроз, расчёт рисков, а также выбора мер направленные на уменьшение и защиту этих рисков.