Аннотация

В рамках данной дипломной работы была рассмотрена тема управления событиями информационной безопасности с помощью системы мониторинга и анализа событий IBM QRadar SIEM.

В результате проведенных работ сформулированы следующие результаты:

а) представлен обзор SIEM системы и краткие характеристики данного продукта;

б) согласовано размещение сервера, установлен гипервизор, собран RAID – массив и настроен удаленный доступ;

в) была определена топология сети и выделены IP-адреса, а также сделана начальная конфигурация IBM QRadar;

г) разработаны и настроены дополнительные правила, настроен парсинг журналов событий, а также расследован инцидент информационной безопасности.