Annotation

As part of this thesis, the topic of information security event management using the IBM QRadar SIEM event monitoring and analysis system was considered.

As a result of the work, the following results are formulated:

а) provides an overview of the SIEM system and brief characteristics of this product;

б) the server location was agreed, a hypervisor was installed, a RAID array was assembled, and remote access was configured;

в) the network topology was determined and IP addresses allocated, and the initial configuration of IBM QRadar was made;

г) additional rules were developed and configured, parsing of event logs was configured, and an information security incident was investigated.