Abstract

The theme of the diploma project is “Organization security management using the system Open Source Security Information Management”. The project was implemented in the company “Просто Бэк-Офис”. In this work, we analyzed the architecture of the SIEM system, investigated and compared various SIEM systems, selected the OSSIM system, and based on it we designed a system for collecting and correlating information security events. Comparison of OSSIM with the paid version of the USM system is shown, a block diagram of the corporate network is developed after the introduction of the system, a «BruteForce» attack was also performed on a host on the network, and the results of the system detection were shown. Also, system tools were examined, such as the host intrusion detection system - OSSEC, the network intrusion detection system - Suricata, the asset scanner - Nagios, the vulnerability scanner - OpenVAS.

Working conditions were analyzed with the calculation of air conditioning and fire safety

Information security risks were calculated, the task of which was to understand real threats, calculate risks, as well as choose measures aimed at reducing, protecting these risks .