Annotation

In the graduation project, a software package was implemented that combines modules for analyzing incidents, rules, encryption, monitoring and creating cross-correlation rules using SearchInform SIEM (System information and Event Management), Data Center. The main priority of this system is the integration (implementation) in the near future and a perfectly suitable medium and small enterprises with a higher level of security to a new level. Joint modules DLP, DataCenter, Web Analytic, Data Report Center - provide information security at all levels and stages of development, and simple integration will instantly connect sources to SIEM. Web Analytic, Data Report - provide an extended map of incidents and possible threats. Investigation of incidents will be fast and fast in real time, allowing you to filter out more important tasks for the organization.