Аңдатпа

Дипломдық жобаның тақырыбы: «Ұйымның қауіпсіздігін Open Source Security Information Management жүйесі арқылы басқару». Жоба «Просто Бэк-Офис» компаниясында жүзеге асырылды. Бұл жұмыста SIEM жүйесінің архитектурасы талданды, әртүрлі SIEM жүйелері зерттелді және салыстырылды, OSSIM жүйесі таңдалып, соның негізінде ақпараттық қауіпсіздік оқиғаларын жинау және өзара байланыстыру жүйесі жасалды. OSSIM-ді жүйесінің ақылы USM нұсқасымен салыстыруы көрсетілген, жүйені енгізгеннен кейін корпоративті желінің блок-схемасы жасалынған, желідегі құрылғыға «BruteForce» шабуылы жасалынған және жүйемен анықталған нәтижелер көрсетілген. Сондай-ақ, жүйенің хосстағы шабуылдарды анықтау жүйесі - OSSEC, желіні басып кіруді анықтау жүйесі - Suricata, активтерді анықтау - Nagios, осалдықты анықтау – OpenVAS сияқты құралдар қарастырылған.

Кондиционерлерді және өрт қауіпсіздігін есептеу кезінде жұмыс жағдайын талдау.

Ақпараттық қауіпсіздіктің қауіп-қатері есептелді, олардың міндеті нақты қауіп-қатерлерді түсіну, қауіп-қатерлерді есептеу, сондай-ақ осы қауіп-қатерлерді азайтуға және қорғауға бағытталған шараларға таңдау жүргізілді.