Аңдатпа

Дипломдық жұмыстың бөлігі ретінде IBM QRadar SIEM оқиғаларын бақылау және талдау жүйесін қолдана отырып, ақпараттық қауіпсіздік оқиғаларын басқару тақырыбы қарастырылды.

Жұмыстың нәтижесінде келесі нәтижелер тұжырымдалады:

а) SIEM жүйесі мен осы өнімнің қысқаша сипаттамаларын ұсынады;

б) сервердің орналасуы келісілді, гипервизор орнатылды, RAID массиві жиналды және қашықтан қол жетімділік конфигурацияланды;

в) желінің топологиясы анықталып, IP мекенжайлары бөлінді және IBM QRadar бастапқы конфигурациясы жасалды;

г) қосымша ережелер жасалды және конфигурацияланды, оқиғалар журналын талдау жасалды, ақпараттық қауіпсіздік оқиғасы зерттелді.