АҢДАТПА

Дипломдық жұмыс «Ақпарат пен оқиғалар қауіпсіздігін басқару жүйесінің (SIEM-система) деректерді жинау және алдын ала өңдеу компонентін құру (жасау)» тақырыбына арналған. Бұл дипломдық жұмыс аса маңызды объектілер бөлімінен, SIEM-жүйесі бөлімінен, бағдарламалық бөлімнен, өмір тіршілік қауіпсіздігі бөлімінен және экономикалық бөлімнен тұрады.

Аталған жұмыста SIEM-жүйесінің компонеттерінің қызметі талданып, қалыпқа келтіру кызметінің функционалына айрықша назар аударылды. Деректерді жинақтаушы бағдарламалар талданып, қалыпқа келтіру қызметі үшін бағдарламалық шешім ұсынылды. Бағдарламалық шешім Python 3.6 бағдарламалық тілінде жазылды. Бағдарламаның негізгі қызметі ретінде әр түрлі дерек көздерінен келген логтарды бір форматқа келтіру болып алынды. Логтарды өңдеуге дейін бірыңғай форматтағы логтарды жеке бөлу қарастырылған.