

## АҢДАТПА

Осы дипломдық жұмыс TLS хаттамасын жүзеге асырудың қауіпсіздігі мәселесіне арналған және TLS протоколын іске асырудың тестілеу әдістемесін әзірлеуге бағытталған. Жұмыс барысында хаттамаға шабуылдар талданды, параметрлер бөлінді, олардың көмегімен шабуылдар іске асырылды. Хаттаманың TLSv1.0, TLSv1.1, TLSv1.2 нұсқалары сыналған тестілеу әдісі жасалды. Тестілеу нәтижелері мен қорғау бойынша ұсыныстар келтірілді.