РЕФЕРАТ

Об’єм роботи 78 сторінок. Робота містить 16 таблиць, 11 рисунків, 1 додаток та 17 літературних посилань.

Об'єктом дослідження є процеси криптографічного захисту електронного голосування, які на даний час є актуальними.

Предметом дослідження є протоколи електронного голосування.

В роботі досліджуються протоколи електронного голосування, методи вибору та оптимізація параметрів.

На основі даних про стійкість асиметричних криптосистем та обчислювальних можливостей різних комп’ютерів, виділено два класи зловмисників в залежності від доступних обчислювальних та інших ресурсів та їхньої можливості вплинути на голосування шляхом злому криптографічних систем захисту.

У роботі аналізується час шифрування, підрахунку та передачі даних для протоколів електронного голосування в залежності від кількості кандидатів, виборців та виборчих дільниць, зокрема, у межах України, враховуючи складність криптографічних алгоритмів та час виконання однієї операції на комп’ютері з вказаним процесором. Введено класифікацію виборів залежно від масштабу та запропоновано деякі рекомендації для проведення голосування.

Проаналізовано протокол електронного голосування, який використовує в своїй основі прості числа, та запропонована модифікація.

Результати роботи можуть бути використані при вибору, побудові та аналізу протоколів електронного голосування.

ПРОТОКОЛИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ, АСИМЕТРИЧНІ КРИПТОСИСТЕМИ, ОБЧИСЛЮВАЛЬНІ МОЖЛИВОСТІ КОМП’ЮТЕРІВ, СКЛАДНІСТЬ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ.