

Анотація

Дипломний проект складається з пояснювальної записки в складі: 82с., 21 рис., 4 табл., 45 літературних джерел.

Мета роботи – розробка та дослідження ефективності методу виявлення атак на основі алгоритмів кластерного аналізу, що передбачає застосування для виявлення атак в реальній мережі.

В процесі виконання роботи було проведено дослідження ефективності застосування різних методів кластерного аналізу для вирішення завдання виявлення мережевих атак, а також розроблено метод виявлення атак, заснованих на алгоритмах кластерного аналізу.

Реалізовано аналізатор системи виявлення мережевих атак оснований на алгоритмах кластерного аналізу. Проведення навчання аналізатора та тестування.

Ключові слова: кластерний аналіз, мережеві атаки, мережевий екран, кластеризація.

Annotation

Thesis consists of: 82 pages, 21 illustrations, 4 tables, 45 literary sources.

Purpose – to develop and study the effectiveness of intrusion detection method based on cluster analysis algorithm that provides intrusion detection for use in a real network.

During the execution of a study of the effectiveness of different methods of cluster analysis to solve the problem of detection of network attacks, and the method of intrusion detection based on cluster analysis algorithms.

Implemented analyzer detection network attacks based on algorithms of cluster analysis. Conducting training analyzer and testing.

Keywords: cluster analysis, network attacks, firewall, clustering.