ABSTRACT ON MASTER'S THESIS

Masters thesis: 106 p. 15 fig., 33 tab.;76 sources.

NETWORK FUNCTION VIRTUALIZATION, INTRUSION DETECTION SYSTEM, NETWORK ATTACKS, MACHINE LEARNING, ANOMALY DETECTION

Topicality: Network Function Virtualization is one of the most promising enterprise networking field cauuse of its abiliity to reduce capital and operating expenses. It is projected that by the end of 2020, the market capitalization will actually be valueable of 15.5 billion dollars. The main unresolved issues of the virtual network functions are the security that is the subject of study of this work. Purpose: The purpose of this work is to improve security in the field of virtual network function by developing intrusion detection system.

Solution: In this paper, the concept of network functions virtualization, information security problems that are relevant to this concept and methods of detection of network attacks as one of the ways to improve the state of security were analyzed and, as a result, an intrusion detection system for Network Function Virtualization was developed.

Object of research: Network Function Virtualization Research subject: Network attack detection methods that can be used in a network infrastructure built on the virtualization of network functions. Scientific Novelty: An attack vector model for virtualization of network functions and an intrusion detection system focused on virtualization of network functions. The practical meaning of the results obtained: The developed system can be used in next-generation networks to protect against network attacks.