РЕФЕРАТ

Актуальність теми. Мережеві технології, на сьогоднішній день, дуже швидко розвиваються. Збільшується швидкість передачі, розмір даних, що зберігаються. Однак, разом з ними, розвиваються і зловмисні системи, які застосовуються для перехвату даних, та/або виведення з ладу каналів передачі даних. Останнім часом зріс інтерес до програмно-конфігурованим мереж SDN (Software-Defined Networks). Перевага представленої технології в тому, що вона працює окремо від мережевих пристроїв, і її контроль може здійснюватися операторами за допомогою стандартного сервера. У з’вязку з таким ростом популярності SDN мереж, проблеми безпеки даних в таких мережах також є актуальними.

Мета роботи — підвищення рівня захищенності програмно-конфігуровних мереж SDN за рахунок розробки модифікованого алгоритму забезпечення завадостійкості та захисту мережі від основних типів атак.

Об’єкт дослідження — методи та алгоритми захисту даних в мережі SDN.

Предмет дослідження — система захисту даних в мережі типу SDN, аналіз існуючих методів та алгоритмів, узагальнена модель мережі типу SDN, обґрунтування вибору методів для підвищення захисту мережі.

Методи досліджень — методи систематизації та формалізації для аналізу існуючих загроз в мережах типу SDN та, відповідно, методів та алгоритмів боротьби з цими загрозами.

Наукова новизна одержаних результатів полягає в тому, що:

1. На основі аналізу типових атак в мережах типу SDN виявлено основні види атак, які можливі в даному типі мереж, розроблена класифікація основних атак на мережу з інформацією, в яких частинах інфраструктури вони можуть проявлятись.
2. Показано, що існуючі підходи не забезпечують достатній рівень захищеності комп’ютерної мережі мережі та робочих станцій в ній.

3. В результаті аналізу методів та алгоритмів попередження (D)DoS-атак на контролер запропонована модифікована версія методу захисту мережі від атак, яка відрізняється додатковим модулем балансувача навантаження між основним та дублюючим контролером.

Практична цінність одержаних результатів полягає в покращенні існуючих методів захисту модулів програмно-конфігуровних мереж SDN, що дозволяє захистити модулі мережі від основних типів атак.

Апробація роботи. Основні положення і результати роботи представлені та обговорені на:

XI конференції молодих вчених «Прикладна математика та комп'ютинг — ПМК-2019» (Київ, 14 – 16 листопада 2019 року);

12 міжнародній науково-практичній конференції «Інтегровані інтелектуальні робототехнічні комплекси — ІІРТК-2019» (Київ, 21 – 22 травня 2019 року).

Публікації.

За результатами магістерської дисертації було опубліковано 2 наукові праці, з них 2 тези доповідей.

Структура та обсяг роботи.

Магістерська дисертація складається зі вступу, трьох розділів, висновків та *N-додатків*.

У *вступі* подано загальну інформацію про поточний стан та актуальність проблеми безпеки SDN-мереж.

В *першому розділі* подана основна теоретична інформація про технологію SDN, наведена класифікація можливих атак в мережах технології SDN.

В *другому розділі* детально проаналізовано існуючі методи боротьби з атаками на контролер.

В *третьому розділі* наведено пропозиції з покращення існуючих алгоритмів захисту мереж SDN. Наведено порівняння існуючих методів для запобігання атак в SDN мережах та вдосконалених методів.

У *висновках* представлені результати проведеної роботи.

Робота представлена на N аркушах, містить посилання на список використаних літературних джерел.

Ключові слова: програмно-конфігуровні мережі, (D)DoS-атаки, SDN-контролер, балансувач навантаження, OpenFlow, SYN-флуд, ARP-спуфінг, система захисту

ABSTRACT

Actuality of theme. Networking technologies are evolving very quickly to date. The transfer speed and the size of the stored data are increasing. However, along with them, malicious systems are being developed that are used to intercept data and / or disable data channels. Recently, interest in Software-Defined Networks (SDN) has increased. The advantage of the presented technology is that it operates separately from network devices, and its control can be exercised by operators using a standard server. Due to the increasing popularity of SDN networks, data security issues in such networks are also relevant.

The purpose of this work is to increase the security level of SDN software and configuration networks by developing a modified algorithm to ensure resilience and protect the network against major types of attacks.

Object — methods and algorithms for data protection on the SDN network.

The subject — of the research is the system of data protection in the network of type SDN, the analysis of existing methods and algorithms, the generalized model of the network of type SDN, the justification of the choice of methods for enhancing the network protection.

Research Methods — systematization and formalization methods for analyzing existing threats in SDN-type networks and, accordingly, methods and algorithms for dealing with these threats.

The scientific novelty of the obtained results is that:

1. Based on the analysis of typical attacks in the SDN type networks, the main types of attacks that are possible in this type of networks were identified, the classification of the main attacks on the network with information in which parts of the infrastructure they could occur.
2. It is shown that the existing approaches do not provide a sufficient level of security for the computer network of the network and the workstations in it.
3. Also, as a result of the analysis of methods and algorithms of (DDoS attacks on the controller, a modified version of the network protection method is

proposed, which has an additional module of load balancer between the main and duplicate controller.

The practical value of the obtained results is to improve of the existing methods of protection of the modules of the software-configuration networks SDN.

Testing the work. The main provisions and results of the work are presented and discussed at:

XI Conference of Young Scientists “Applied Mathematics and Computing - PMK-2019” (Kyiv, November 14 - 16, 2019);

12th International Scientific-Practical Conference "Integrated Intelligent Robotics Complexes - IIRTK-2019" (Kyiv, May 21 - May 22, 2019).

Publications.

According to the results of the master's thesis, 2 scientific works were published, 2 of which were abstracts.

Structure of work.

The *master's* thesis consists of an introduction, three sections, conclusions and N-applications.

The *introduction* provides general information about the current status and current security issues of SDN networks.

The *first* section provides basic theoretical information about SDN technology, and provides a classification of possible attacks in SDN technology networks.

The *second* section actually analyzes the existing methods of controlling attacks against the controller.

In *third* section had been provided suggestions for improving existing SDN security algorithms. Comparison of existing methods for preventing attacks on SDN networks and advanced methods is presented.

The *results* of the work carried out are presented in the conclusions.

The work is presented on N worksheets, containing links to the list of used literature sources.

Keywords: software-defined networks, (D)DoS-attacks, SDN-controller, load balancer, OpenFlow, SYN-flood, ARP-spuffing, security system