UDC 004.7.056.5

V. TKACH
Blekinge Institute of Technology, Karlskrona, Sweden; National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute,” Kyiv, Ukraine,
e-mail: *volodymyr.tkach@bth.se, vntkach@gmail.com.*

A. KUDIN
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute;” National Bank of Ukraine, Kyiv, Ukraine,
e-mail: *pplayshner@gmail.com.*

V. ZADIRAKA
V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Kyiv, Ukraine,
e-mail: *zvk140@ukr.net.*

I. SHVIDCHENKO
V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Kyiv, Ukraine,
e-mail: *inetsheva@gmail.com.*

SIGNATURELESS ANOMALOUS BEHAVIOR DETECTION IN INFORMATION SYSTEMS

Abstract. The early detection of cyber threats with cyber-attacks adapted to the nature of information systems is a crucial cybersecurity problem. This problem and the task of recognizing normal and abnormal states and behavior of various processes in information systems are closely related. An additional condition is often the absence of templates, signatures, or rules of normal behavior that would allow using existing statistical or other known methods of data analysis. We analyze the existing and propose a new method for detecting abnormal behavior without the use of signatures based on the finite state machine (FSM) model and the Security Information and Events Management (SIEM) system.

Keywords: anomaly detection, finite state machine, SIEM, time-series, cybersecurity.

INTRODUCTION

The increasing impact of cyber threats on critical infrastructure is attributable to the simultaneous rise of information flows and infrastructure complexity. Higher complexity often results in higher functionality, which, in turn, reduces the security level of any system, as has been established [1].

As the number of cyber-attacks continues to rise [2], safeguarding critical infrastructure objects [3], which are mostly state institutions, becomes the top priority for cyber defense. It is widely recognized that modern cyber-attacks are becoming increasingly sophisticated and causing significant damage to their targets. In recent times, several highly sophisticated supply chain attacks have been witnessed, which may have had a multi-step history and could have been detected at early stages if a method for detecting anomalous behavior was available.

A significant issue in cyber defense is the absence of effective mechanisms for detecting and preventing attacks unless specific attack patterns or even signatures are identified. As a result, the development of pre-detection and prevention mechanisms for cyber threats has become crucial, particularly in cases where there is insufficient information about potential threats and their signatures. Such mechanism should be based on identifying anomalies in user behavior, where an anomaly refers to unusual user behavior that deviates from what is expected rather than the “normal” behavior. It is important to note that what is considered normal can be subjective and varies across different systems. Forecasting will be the primary method for identifying deviations from expected behavior.

To sum up the above-mentioned, modern cybersecurity is defined on the one hand by the changeable character of threats, and on the other hand, by adaptive change of the very state of specific information system in cyberspace, which is considered as safe. Traditional information security technologies are built in the