https://orcid.org/0000-0002-5523-6120
https://orcid.org/0000-0002-9176-1256

UDC 004.9

S.V. HOLUB[*], O.M. MYKHAILYK[**]

MODEL SYNTHESIZER FOR CYBERATTACK MONITORING SYSTEM

[*]Cherkasy State Technological University, Cherkasy, Ukraine
[**]Institute of Mathematical Machines and Systems Problem National Academy of Sciences of Ukraine, Kyiv, Ukraine

Анотація. *У статті описано метод моніторингу стану безпеки локальних корпоративних мереж, який об'єднує процеси синтезу та аналізу моделей поведінки вхідних даних, прогнозування їх значень і моделювання процесів кібератак. Створено моделі-класифікатори кіберзагроз. Характеристики потоків даних надходять у мережу за допомогою датчиків, встановлених у заздалегідь запланованих точках-пастках комп'ютерної мережі. Відбувається класифікація векторів із показників, що характеризують ці кібератаки. Отримані результати представлені у вигляді кількісних і якісних оцінок відповідно до основних положень теорії складних систем. Для підвищення ефективності захисту мережі було запропоновано централізувати обчислювальний процес із використанням грід-інфраструктури та хмарної платформи. Проведено попереднє порівняння грід і хмарної технологій. Трудомістка і обчислювально складна процедура переноситься з локальних обчислювальних мереж у високопродуктивні середовища. За допомогою імітаційних моделей було проведено дослідження змін станів схеми обробки запитів, виходячи з вибірки атак, що надійшли до комп'ютерних систем. Модель, при надходженні вхідних потоків даних, враховує їх вид, а також інтенсивність, запобігаючи використання однотипних атак для здійснення задуманої зловмисником схеми, таким чином нейтралізуючи їх вплив, дозволяючи аналізувати більш складні види кібератак. Крім кібербезпеки, прискорення завдання множинного розпізнавання є актуальним і для багатьох інших важливих додатків, таких як інтелектуальний аналіз даних, прискорена обробка XML-запитів, управління технологією QoS, фільтрація в IP-телефонії, оптимізація кешування тощо.*

Ключові слова: *синтезатор моделей, кібератаки, система моніторингу.*

Аннотация. *В статье описан метод мониторинга состояния безопасности локальных корпоративных сетей, объединяющий процессы синтеза и анализа моделей поведения входных данных, прогнозирования их значений и моделирования процессов кибератак. Созданы модели-классификаторы киберугроз. Характеристики потоков данных поступают в сеть с помощью датчиков, установленных в заранее запланированных точках-ловушках компьютерной сети. Происходит классификация векторов из показателей, характеризующих эти кибератаки. Полученные результаты представлены в виде количественных и качественных оценок в соответствии с основными положениями теории сложных систем. Для повышения эффективности защиты сети было предложено централизовать вычислительный процесс с использованием грид-инфраструктуры и облачной платформы. Проведено предварительное сравнение грид и облачной технологий. Трудоемкая и вычислительно сложная процедура переносится с локальных вычислительных сетей в высокопроизводительные среды. С помощью имитационных моделей было проведено исследование изменений состояний схемы обработки запросов, исходя из выборки поступивших атак в компьютерные системы. Модель, при поступлении входных потоков данных, учитывает их вид, а также интенсивность последних, предотвращая использование однотипных атак для осуществления задуманной злоумышленником схемы, таким образом нейтрализуя их воздействия, позволяя анализировать более сложные виды кибератак. Кроме кибербезопасности, ускорение задачи множественного распознавания актуально и для многих других важных приложений, таких как интеллектуальный анализ данных, ускоренная обработка XML-запросов, управление технологией QoS, фильтрация в IP-телефонии, оптимизация кэширования и т.д.*

Ключевые слова: *синтезатор моделей, кибератаки, система мониторинга.*

Abstract. *The paper describes a method of monitoring the security status of local corporate networks, which combines the processes of synthesis and analysis of input behavior patterns, prediction of their values and modeling of cyberattacks. Model-classifiers of cyber threats have been created. Characteristics of data flows come into the network with the help of sensors installed in advance scheduled trace points of the computer network. There is a classification of vectors from the indicators that characterize these cyber attacks. The obtained results are presented both quantitatively and qualitatively, in accordance with the basic provisions of the theory of complex systems. In order to increase the efficiency of network protection, it was proposed to centralize computational process using grid infrastructure and cloud platform. A preliminary comparison of grid and cloud technologies has been carried out. The workload and computationally complicated procedure is transferred from local computer networks to high-performance environments. Using simulation models, it was investigated changes in the state of the query processing scheme, based on a sample of attacks that came to computer systems. The model takes into account heterogeneous input data flows and the possibility of changing the intensity of requests in information systems by attackers, which allows choosing ways to counteract and neutralize the effects of their impact, and analyze more complex cyberattacks. With the help of simulation models, the dynamics of changes in the conditions of the subsystem blocking queries in the process of recognition of cyber attacks in critical computer systems is researched. In addition to cybersecurity, accelerating the task of multiple recognition is relevant to many other important applications, such as intelligent data analysis, accelerated processing of XML queries, QoS technology management, IP-telephony filtering, caching optimization, etc.*

Keywords: *model synthesizer, cyberattacks, monitoring system.*

DOI: 10.34121/1028-9763-2020-1-94-98

1. Introduction

The rapid development of scientific and technological progress in the early 21st century in the field of information technology (IT technologies) is associated with the widespread introduction of them into all areas of the modern society of any developed state of the world. The high pace of informatization of Ukrainian society and state institutions contributes to the further growth of the role and place of cyberspace in the issues of ensuring national security in the information sphere. Cyberspace today is a system-forming factor, whose security not least determines the level of information security of the state.

The mass availability of IT technologies offers wide opportunities for unauthorized access to state information resources for unauthorized users and criminal groups, which creates preconditions for security threats in the national segment of cyberspace in the information sphere [1]. Countering such threats is a fundamental aspect of strengthening the strategic stability of the state and its information security [2]. An incident in information security related to massive cyber-attacks on state information resources, held in February 2012 in the national segment of cyberspace, unprecedented in world practice by its counterparts and implications for state authorities, prompts the revision of existing concepts of building information security systems and strategies for their effective use.

2. The analysis of recent researches and publications

The analysis of recent researches and publications [1–5] allowed to establish one of the priority directions of increasing the level of protection of information resources in particular, and further stabilization of information security of the state as a whole. It consists in a qualitatively new solution to the problem of state information security by creating modern methods and means of protecting information from cyber-attacks, which implement unauthorized access to information resources of information and telecommunication systems and technical objects of their infrastructure. Thus, significant scientific results in solving the problem of information security of the state and the disclosure of its separate components were obtained in scientific works [1–3, 6–

11], etc. However, despite this, the problem remains relevant not only for Ukraine but also for the whole world the community.

Proceeding from the unified system positions [12, 13] and the need to implement an integrated approach to building progressive systems of information security at the present stage of the development of science and technology, there is an objective contradiction between the high requirements put forward to ensure the security of information resources in conditions of information conflict during implementation of the processes of cyber-attack, and the fundamental impossibility of their implementation on the basis of modern information security practices based on obsolete models and methods. In addition, the lack of a common methodological basis further exacerbates the problem of information security. Thus, the further development of mathematical tools for studying the problem of the state information security is an urgent scientific task that needs to be addressed.

In this regard, the purpose of the article is to develop an appropriate methodology for the synthesis and analysis of models and methods for modeling the processes of cyber-attacks, necessary and sufficient for solving a number of practical problems of information security.

3. Basic research materials

It is known [9] that the basis of mathematical models and methods for modeling the processes of cyber-attack is based on three basic approaches – theoretical, empirical and theoretical-empirical. The aforementioned approaches are based on the methods of such theories: support and decision making, sets, graphs, games, perturbations, probabilities, Petri networks and semi-Markov processes, as well as methods of matrix and economic analysis, neural networks and Markov chains, optimization methods, logic and traffic theory. A grouping of a definite mathematical toolkit has made it possible to establish that all known models based on the above methods can be classified into three main classes – static, stochastic and dynamic. [11] shows that the application of known models allows obtaining quantitative, qualitative and quantitative qualitative estimates of the level of protection of information resources, but in practice these models are limited to assessing the predicted level of security, since its unjustified overestimation or understatement can lead to significant financial costs. At the same time, the overwhelming majority of models and methods are designed to simulate the processes of cyber defense. Thus, as it is clear from the foregoing, on the basis of the existing methodological apparatus it is difficult to achieve the objective set forth in the article. For the completeness of describing the processes of cyber-attack in modern conditions it is advisable to apply a fundamentally new modeling concept based on the synthesis of methods and models based on the base of algorithms for model synthesis.

According to the results of the patent search, the critical analysis of protected dissertations, monographs on the topic defined in the article, available from open print, it was established that to date, in the field of state information security, such a modeling concept and, accordingly, mathematical tools have not been used before, what determines the scientific priority of the study. The effectiveness of modeling the processes of cyber-attack using methods of synthesis theory of models using synthesis algorithms is due to a number of circumstances [13]. Part of models and methods of simulation based on neural networks, methods of taking into account group arguments, genetic algorithms, etc. open the possibility of research on the development of the dynamics of cyber-attacks, their randomized origin are taken into account, and also adequately reflect the antagonism of the interests of the subject. The antagonism generated by the contradiction between the interests and goals of the players is the source of the information conflict. Information Conflict, as a systemic phenomenon, is characterized by structural, dynamic and game-theoretical properties, neglecting any of which – it is impossible. The use of a synthesizer of models and simulation techniques will, in practice, result in the development of effective preventive measures aimed at protecting information. Unlike other operating methods, such as Laplace integral transformations, Mellin, Fourier, etc., the modeling

area is not limited to linear equations. The property of the system's adaptability to the choice of the form of modeling increases the efficiency of the methods of synthesis and analysis of information security systems, as well as the simulated processes. The lack of methodological error ensures the reliability of the methods and the adequacy of the models to the actual processes. Possibility of obtaining analytical models using the method of various algorithms for model synthesis opens new ways for the introduction into practice of protection of a wide class of progressive systems of information security. Mathematical modeling of application data protection problems by such methods is based on the observance of such factors, which verbal level determines the essence of this theory.

Based on the well-known approach to the construction of methodologies [13], the article, on the basis of research, proposes a methodology for the creation of instruments for synthesizer models and methods for modeling the processes of cyber-attack using a database of algorithms for the synthesis of models:

1. Determining the set of states of the information security system.
2. Selection of strategies for cyber defense (neural network, algorithm of the method of group consideration of arguments, etc.).
3. Optimization of cyber defense strategies and security assessment.
4. Forecasting the development of the dynamics of the process of cyber-attack.
5. Optimization of cyber defense resources and security assessment.
6. Evaluation of the effectiveness of the information security system.

4. Conclusions

On the basis of the proposed methodology of synthesis and analysis of the models formed by the synthesizer models and methods for modeling the processes of cyberspace, it is possible to build both software and hardware-based information security systems integrated into newly created technologies that are designed to provide in real time the predicted level of protection of information resources from the cyberattack of the predicted class. The application of the methodology also provides the choice of the best option for the construction of a progressive information security system based on an integrated system performance indicator based on developed models and simulation methods. Based on the synthesizer of models and methods of analysis of different types of algorithms, the methodology allows to assess the current and projected level of protection, as well as provides prediction of the development of the dynamics of the process of cyber-attack, during which the current level will correspond to the given, which will facilitate the selection of preventive strategies of cyber threats, adequate conditions for the occurrence of information conflicts in systems information security.

REFERENCES

1. Хорошко В.О. Информационная безопасность Украины. Основные проблемы и перспективы. *Захист інформації*. 2008. № 40. С. 6–9.
2. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации: монография. К.: Ариус, 2008. Т. 2: Информационная безопасность. 344 с.
3. Марущак А.І. Інформаційне право. Доступ до інформації: навч. посіб. К.: КНТ, 2007. 532 с.
4. Голубев В.А. Информационная безопасность: проблемы борьбы с киберпреступностью: монография. Запорожье: ГУ «ЗИГМУ», 2003. 336 с.
5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы информационной безопасности. М.: Горячая линия, Телеком, 2004. 280 с.
6. Андон П.І., Ігнатенко О.П. Атаки на відмову в мережі Інтернет: опис проблеми та підходів щодо її вирішення. К., 2008. 50 с.
7. Богуш В.М., Юдін О.К. Інформаційна безпека держави. К.: МК-Прес, 2005. 432 с.
8. Домарев В.В. Информационные технологии безопасности. Системный подход. К.: ООО «ТИД» ДС», 2004. 992 с.

9. Кобозєва А.А. Аналіз стану й технології функціонування систем захисту інформації на основі теорії збурень: автореф. дис. ... д-ра техн. наук спец.: 05.13.21. К.: Держ. ун-т інформаційно-комунікаційних технологій, 2008. 40 с.
10. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем / ред. академіка Національної академії наук України М.З. Згуровського. К.: Видавнича група BHV, 2009. 608 с.
11. Голубенко О.Л. та ін. Політика інформаційної безпеки. Луганськ: Вид. СНУ ім. В. Даля, 2009. 300 с.
12. Корченко О.Г. Системи захисту інформації: монографія. К.: НАУ, 2004. 264 с.
13. Корченко А.Г. Построение систем информационной безопасности на нечетких множествах. Теория и практические решения: монография. К.: МК-Пресс, 2006. 320 с.

Стаття надійшла до редакції 08.07.2019