DOI: 10.37791/2687-0649-2023-18-2-85-102

Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления

***А.Ю. Пучков*[1*], *А.М. Соколов*[1], *С.С. Широков*[2], *Н.Н. Прокимнов*[3]**
[1]*Филиал Национального исследовательского университета «МЭИ» в г. Смоленске, Смоленск, Россия*
[2]*Департамент цифрового развития Смоленской области, отдел защиты информации, Смоленск, Россия,*
[3]*Университет «Синергия», Москва, Россия*
[*]*putchkov63@mail.ru*

Аннотация. Представлены результаты исследований, целью которых была разработка алгоритма выявления угроз информационной безопасности в распределенных мультисервисных сетях, обеспечивающих информационное взаимодействие региональных органов государственного управления, а также их коммуникацию с населением региона. Актуальность темы исследований обусловлена значительным ростом кибератак различных видов на вычислительные сети органов государственной власти и необходимостью повышать уровень защищенности этих сетей за счет интеллектуализации методов борьбы с угрозами информационной безопасности. В основе алгоритма лежит применение методов машинного обучения для анализа входящего трафика с целью выявления событий, влияющих на состояние информационной безопасности органов государственной власти. Алгоритм предусматривает препроцессинг входного трафика, в результате которого формируется набор изображений (сигнатур), получаемых на основе бинарных файлов Wasm, а затем запускается классификатор изображений. Он содержит последовательное включение глубоких нейронных сетей – сверточной нейронной сети для классификации сигнатур и рекуррентной сети, которая обрабатывает последовательности, получаемые на выходе сверточной сети. Особенности формирования сигнатур в предлагаемом алгоритме, а также последовательностей на входе в рекуррентную сеть дают возможность получать результирующую оценку информационной безопасности с учетом предыстории текущего ее состояния. Выход рекуррентной сети агрегируется с результатом сравнения актуальных сигнатур с имеющимися в базе данных. Агрегация выполняется системой нечеткого вывода второго типа, использующей импликацию по алгоритму Мамдани, которая и вырабатывает итоговую оценку угроз информационной безопасности. Разработано программное обеспечение, реализующее предложенный алгоритм, проведены эксперименты на синтетическом наборе данных, которые показали работоспособность алгоритма, подтвердили целесообразность его дальнейшего совершенствования.

Ключевые слова: распределенные мультисервисные сети, информационная безопасность, глубокие нейронные сети

Для цитирования: *Пучков А.Ю., Соколов А.М., Широков С.С., Прокимнов Н.Н.* Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления // Прикладная информатика. 2023. Т. 18. № 2. С. 85–102. DOI: 10.37791/2687-0649-2023-18-2-85-102

Algorithm for identifying threats to information security in distributed multiservice networks of government bodies

A. Puchkov[1*]***, A. Sokolov***[1]***, S. Shirokov***[2]***, N. Prokimnov***[3]
[1]*Branch of the National Research University "MPEI" in Smolensk, Smolensk, Russia*
[2]*Digital Development Department of the Smolensk Region, Information Security Department, Smolensk, Russia,*
[3]*Synergy University, Moscow, Russia*
[*]*putchkov63@mail.ru*

Abstract. The results of studies are presented, the purpose of which was to develop an algorithm for identifying information security threats in distributed multiservice networks that provide information interaction of regional government bodies, as well as their communication with the population of the region. The relevance of the research topic is due to a significant increase in various types of cyber attacks on the computer networks of public authorities and the need to increase the level of security of these networks by intellectualizing methods for combating information security threats. The algorithm is based on the use of machine learning methods to analyze incoming traffic in order to identify events that affect the state of information security of public authorities. The algorithm provides for input traffic preprocessing, as a result of which a set of images (signatures) obtained from Wasm binary files is formed, and then the image classifier is launched. It contains a sequential inclusion of deep neural networks – a convolutional neural network for signature classification and a recurrent network that processes the sequences obtained at the output of the convolutional network. Features of the formation of signatures in the proposed algorithm, as well as sequences at the input to the recurrent network, make it possible to obtain the resulting assessment of information security, taking into account the history of its current state. The output of the recurrent network is aggregated with the result of comparing the actual signatures with those available in the database. The aggregation is performed by the fuzzy inference system of the second type, using the implication according to the Mamdani algorithm, which generates the final assessment of information security threats. Software was developed that implements the proposed algorithm, experiments were carried out on a synthetic data set, which showed the efficiency of the algorithm, confirmed the feasibility of its further improvement.

Keywords: distributed multiservice networks, information security, deep neural networks

For citation: Puchkov A., Sokolov A., Shirokov S., Prokimnov N. Algorithm for identifying threats to information security in distributed multiservice networks of government bodies. *Prikladnaya informatika*=Journal of Applied Informatics, 2023, vol.18, no.2, pp.85-102 (in Russian). DOI: 10.37791/2687-0649-2023-18-2-85-102

Введение

В сложных современных условиях противостояния на международной арене Российской Федерации и Западного мира их конфронтация в подавляющем большинстве сфер взаимодействия делает задачу повышения уровня национальной безопасности России одним из приоритетных направлений деятельности органов государственной власти разных уровней. В рамках этой задачи должна обеспечиваться и информационная безопасность (ИБ) страны как один из важнейших элементов деятельности целого стека органов власти: Комитета Государственной Думы по безопасности; Совета безопасности России; Федеральной службы по техническому и экс-