УДК 004.93'14
DOI: 10.25559/SITITO.18.202204.872-877

Оригинальная статья

Обнаружение низкоинтенсивных DoS атак с помощью применения комбинированной нейронной сети с использованием алгоритма анализа уровня DoS атаки

А. С. Турашев[1*], В. А. Сухомлин[1,2]
[1] ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», г. Москва, Российская Федерация
Адрес: 119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1
*turashev.artem@mail.ru
[2] ФГУ «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Российская Федерация
Адрес: 119333, Российская Федерация, г. Москва, ул. Вавилова, д. 44-2

Аннотация
Рост количества и сложности атак на доступ к информации – это одна из основных проблем в сфере web-преступлений сегодня. Эти вторжения образуют класс атак типа «отказ в обслуживании». DoS атака – атака, осуществляемая для того, чтобы довести систему до отказа в работе. Происходит генерация огромного количества трафика, из-за которого происходит перезагрузка сервера, что в дальнейшем приводит к его блокировке. Обычно часто атакуемыми ресурсами являются: ширина канала, процессорное время серверов и роутеров и пр. В целях минимизации последствий таких атак применяется широкий набор механизмов. Одним из этих средств является метод обнаружения вторжений. Однако, при выявлении низкоинтенсивных атак (low-rate-DoS) некоторые способы обнаружения атак, основанные на стандартных статистических методах, показывают достаточно низкий результат. В данной ситуации нейронные сети выступают в качестве решения проблемы. Они используются практически во всех средствах обнаружения атак как отдельно, так и с другими механизмами защиты. В данной статье приведено описание разработки и экспериментальное исследование эффективности метода обнаружения низкоинтенсивных атак типа отказ в обслуживании (low-rate-DoS) и внедрение в него разработанного алгоритма анализа уровня DoS атаки. В приведенной работе используется модель низкоинтенсивных атак в виде одновременного наложения сетевых событий и аномального трафика. Суть метода заключается в выделении однородных групп временного ряда с помощью моделей распознавания образов и построения для каждой конкретной группы модели прогнозирования для обнаружения сценария атаки.

Ключевые слова: низкоинтенсивная DoS атака, обнаружение атак, нейронная сеть, сетевая безопасность

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Турашев А. С., Сухомлин В. А. Обнаружение низкоинтенсивных DoS атак с помощью применения комбинированной нейронной сети с использованием алгоритма анализа уровня DoS атаки // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 4. С. 872-877. doi: https://doi.org/10.25559/SITITO.18.202204.872-877

Original article

Detection of Low-Intensity DoS Attacks by Using a Combined Neural Network Using a DoS Attack Level Analysis Algorithm

A. S. Turashev[a*], **V. A. Sukhomlin**[a,b]
[a] Lomonosov Moscow State University, Moscow, Russian Federation
Address: 1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation
[*] turashev.artem@mail.ru
[b] Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russian Federation
Address: 44 Vavilov St., building 2, Moscow 119333, Russian Federation

Abstract
The growing number and complexity of attacks on access to information is one of the main problems in the field of web crimes today. These intrusions form a class of denial-of-service attacks. DoS attack is an attack carried out in order to bring the system to failure. A huge amount of traffic is generated due to which the server is rebooted, which further leads to its blocking. Usually, the most frequently attacked resources are: channel width, processor time of servers and routers etc. In order to minimize the consequences of such attacks, a wide range of mechanisms are used. One of these tools is the intrusion detection method. However, when detecting low-intensity attacks (low-rate-DoS), some methods of detecting attacks based on standard statistical methods show a rather low result. In this situation, neural networks act as a solution to the problem. They are used in almost all attack detection tools, both separately and with other protection mechanisms. This article describes the development and experimental study of the effectiveness of the method for detecting low-intensity denial-of-service attacks (low-rate-DoS) and the implementation of the developed algorithm for analyzing the level of DoS attacks. This paper uses a model of low-intensity attacks in the form of simultaneous overlay of network events and abnormal traffic. The essence of the method is to identify homogeneous groups of a time series using pattern recognition models and build a prediction model for each specific group to detect an attack scenario.

Keywords: low-intensity DoS attack, attack detection, neural network, network security

Conflict of interests: The authors declare no conflict of interest.

For citation: Turashev A.S., Sukhomlin V.A. Detection of Low-Intensity DoS Attacks by Using a Combined Neural Network Using a DoS Attack Level Analysis Algorithm. *Modern Information Technologies and IT-Education.* 2022;18(4):872-877. doi: https://doi.org/10.25559/SITITO.18.202204.872-877

Введение

На сегодняшний день обнаружение DoS атак является достаточно непростой задачей, потому что не существует общих признаков, по которым можно было бы сразу определить цель запроса к ресурсам сервера. Работа информационных систем и сети зависит не только от степени надежности используемой аппаратуры, но и от способности сети противостоять действиям атакующего. Каждый день выявляется все больше новых способов организации DoS атак, и многие существующие методы защиты уже, к сожалению, не могут противостоять им.

Цель исследования

Целью данной работы является рассмотрение и изучение комбинированного нейросетевого метода обнаружения низкоинтенсивных атак типа отказ в обслуживании (low-rate-DoS) и внедрение разработанного алгоритма анализа уровня такой DoS атаки в него.

Модель низкоинтенсивной атаки типа отказ в обслуживании (low-rate-DoS)

Сетевой трафик представляет множество пакетов, проходящих по каналам связи. Для того, чтобы обнаружить атаку, необходимо определить появление определенного набора пакетов. После этого обнаружения необходимо отнести этот набор либо к нормальному, либо к аномальному классу (в данном случае под аномалией будем подразумевать наличие низкоинтенсивной атаки). Порядок следования пакетов не будет оказывать особого значения для обнаружения атаки. Информация о времени, когда пришли эти пакеты, будет учитываться при разбиении входящего трафика на «окна» [1-8].

Для обнаружения атаки рассмотрим задачу разработки классификатора наборов сетевых пакетов, который будет помечать метками наши наборы пакетов для временного ряда элементов $\alpha_1,...,\alpha_{i-1},\alpha_i$:

$$\eta(\alpha_1,...,\alpha_{i-1},\alpha_i)=\begin{cases}C^S : s_i^{'} \neq 0,\\ C^d : d_i^{'} \neq 0\end{cases}$$

где η - длина истории событий; α_i - событие, представляющее вектор атрибутов события, то есть $\alpha_i =< x_j^i : j = 0..M-1 >$, где M – количество рассматриваемых атрибутов.

Таким образом, мы получаем, что наша задача сводится к классификации многомерных временных рядов. Для данной задачи будем применять альтернативный подход к классификации временных рядов. Его главные особенности заключаются в следующем:

1. Для выделения признаков используется скользящее окно;
2. Обучение классификатора происходит только для окна[1].

Пусть $\exists$ ряд $A=\{a_i\}$, $i=0..N-1$. В нашем случае N это длина временного ряда. Поделим этот ряд на некоторые участки (окна) G, каждое из которых будет являться вектором определенной длины. Длина окна в нашем случае – это длина истории событий X.

$$\begin{aligned}&m=0;\\ &for\ (int=0;\ i<N\ -\ 1;\ ++i)\{\\ &\quad G^m_{i \bmod X}=\alpha_i;\\ &\quad if\ \ i\ \%\ X == X-1\\ &\qquad ++m;\\ &\}\end{aligned}$$

Алгоритм 1. Данный алгоритм представлен на C++ подобном модельном ЯП

Algorithm 1. This algorithm is presented in C++ similar model programming language

Основная проблема при решении поставленной задачи заключается в том, что элемент классифицируемого временного ряда представлен в виде вектора $\alpha_i =< x_j^i : j = 0..M-1 >$, где M – количество рассматриваемых атрибутов. Вектора, полученные при «развертывании» многомерного временного ряда, будут иметь размерность $|G_m| = X \cdot M$. Это приводит к возрастанию вычислительной сложности метода. Для того, чтобы избавиться от этого недостатка, предлагается использовать методы снижения размерности данных, которые приведены в следующих работах[2] [9-11].

Метод обнаружения низкоинтенсивной атаки типа отказ в обслуживании (low-rate-DoS)

Как и многие методы машинного обучения, данный метод может быть представлен в виде двух фаз – фазы обучения и фазы классификации.

В фазе обучения происходит построение классификатора путём итерационной настройки параметров на обучающей выборке. Иными словами, алгоритм использует часть данных, обрабатывает их, замеряет эффективность обработки и автоматически регулирует свои параметры (также называемый метод обратного распространения ошибки) до тех пор, пока не сможет последовательно производить желаемый результат с достаточной достоверностью. Затем происходит оценка полученных данных на тестовой выборке. В случае, если результат проверки обученного классификатора на тестовой выборке совпадет с ожидаемым результатом, происходит переход к этапу классификации. Целью этого этапа является вычисление меток классов для ранее неизвестных наборов данных с применением обученного классификатора [12-15].

В фазе классификации используется самоорганизующаяся карта (самоорганизующаяся карта Кохонена). Это нейронная сеть,

[1] Haykin S. Neural Networks: A Comprehensive Foundation. 2nd ed. Upper Saddle River, New Jersey : Prentice Hall, 1999. 842 p.

[2] Fodor I. K. A Survey of Dimension Reduction Techniques. Technical Report UCRL-ID-148494. U.S. Center for Applied Scientific Computing, Lawrence Livermore National Laboratory, 2002. 26 p. URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1dc8cf5cdda60f0e6098291266390f6e65c90322 (дата обращения: 11.07.2022).

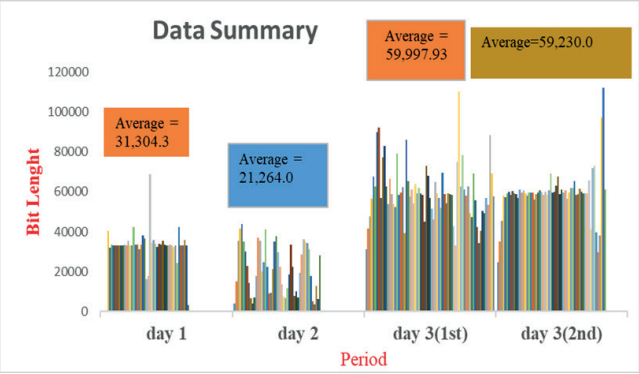
выполняющая задачу визуализации и кластеризации[3]. Эта разработка была предложена учёным Т. Кохоненом, является методом проецирования многомерного пространства в пространство с более низкой размерностью [16]. На вход этой карты последовательно подаются вектора из текущего окна. На выходе получается вектор следующего вида: $< N_1, N_2, ..., N_i >$, где i - индекс, определяющийся размером окна, а N_i указывает на то, к какому кластеру принадлежит данный пакет. Затем этот вектор подается на вход многослойного персептрона. Персептрон анализирует каждое окно и классифицирует его как норму или аномалию (атаку).

Метод будет состоять из следующих шагов:

1. Произвести построение отдельной нейронной сети для каждого сервиса, который нуждается в контроле.
2. Принять в выбранном сервисе от источника некоторое множество сетевых пакетов, число которых будет определяться размерами окна.
3. Произвести снижение размерности входных данных.
4. Сформировать вектора для многослойного персептрона, где каждый компонент вектора будет соответствовать номеру кластера, в который происходит распределение пакета.
5. Провести анализ, в результате которого будет происходить классификация данных и соотнесение их либо к нормальному, либо к аномальному классу[4] [17-19].

Алгоритм анализа уровня DoS атаки

После получения всех пакетов необходимо собрать всю возможную информацию о них. Важно определить такие параметры, как время получения пакетов и длину каждого пакета. На практике воздействие атак измеряется путем дифференциации размеров атаки.



Р и с. 1. Средние значения длин пакетов, собранных за 3 дня

F i g. 1. Average packet lengths collected in 3 days

На рисунке 1 показаны средние значения длин всех полученных пользователем пакетов, которые поступали в разное время в зависимости от загрузок злоумышленников. Анализируя среднюю длину пакетов и вычисляя квартили[5], пользователи имеют возможность определить и понять уровень атак с помощью следующих формул:

$Q_N = (D_{max} - D_{min})$, где $N = 1,2,3,4$, D_{max} = максимальное среднее значение длины пакетов (59997.97 ≈ 59998 бит), D_{min} – минимальное среднее значение длины пакетов (21264 бит). Следовательно, *Range* (диапазон) бит = 59998 – 21264 = 38734 бит.

$$Quartile = \frac{Range}{4} = \frac{38734}{4} \approx 9684 \text{ бит.}$$

Q_1 = от 21264 до (21264 + (1*9684)) бит = от 21264 до 30948 бит

Q_2 = от 30949 до (21264 + (2*9684)) бит = от 30949 до 40631 бит

Q_3 = от 40632 до (21264 + (3*9684)) бит = от 40632 до 50315 бит

Q_4 = от 50316 до (21264 + (4*9684)) бит = от 50316 до 59998 бит

Таблица 1 описывает характеристики собранных пакетов из потока: период, в течение которого эти пакеты были получены (секунды), среднее значение длины пакетов (количество бит), номер квартили (Q_i) и уровни низкоинтенсивной DoS атаки. С помощью квартили (Q_1, Q_2, Q_3 и Q_4), пользователь может легко классифицировать уровень атак (соответственно, как низкий, средний, повышенный и высокий) [20-23].

Т а б л и ц а 1. **Характеристики собранных пакетов из потока**

T a b l e 1. **Characteristics of collected packets from a stream**

Номер сбора пакетов	Время прихода пакетов	Период, в течение которого пришли пакеты, сек	Среднее значение длины пакетов, бит	Номер квартили	Уровень атаки
1	06:59	48	31304.3	Q2	Средний
2	14:01	48	21264.0	Q1	Низкий
3	14:27	71	59997.93	Q4	Высокий
4	10:34	60	59230.0	Q4	Высокий

Приведенная выше таблица иллюстрирует уровень атак. Злоумышленники могут атаковать систему, используя небольшие пакеты с большим количеством загрузок; эти злоумышленники заставляют целевую систему потреблять слишком много ресурсов пропускной способности сети и делают некоторые сервисы недоступными для простых пользователей. Анализируя время атаки и размер всех данных, пользователи могут определить уровень атак.

[3] Жжонов В. А., Евсина В. А., Широбокова С. Н. К вопросу использования самоорганизующейся карты Кохонена для обработки анализируемых данных // Инженерный вестник Дона. 2022. № 7(91). С. 200-206. URL: https://elibrary.ru/item.asp?id=49408176 (дата обращения: 11.07.2022).

[4] Тарасов Я. В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Вопросы кибербезопасности. 2017. № 5(24). С. 23-29. doi: https://doi.org/10.21681/2311-3456-2017-5-23-29

[5] Тюрин Ю. Н., Макаров А. А., Симонова Г. И. Теория вероятностей. М. : МЦНМО, 2009. 256 с. URL: https://elibrary.ru/item.asp?id=21555601 (дата обращения: 11.07.2022); Бондаренко П. С., Горелова Г. В., Кацко И. А. Теория вероятностей и математическая статистика. М. : КНОРУС, 2019. 390 с. URL: https://elibrary.ru/item.asp?id=41558886 (дата обращения: 11.07.2022).

Экспериментальное исследование, полученные результаты и оценка эффективности разработанного метода

В данном эксперименте используется персептрон с двумя открытыми слоями с числом нейронов 21 и 7. Функция активации в скрытых слоях – тангенс гиперболический, а в выходном – линейная. Метод обучения – trainlm [24, 25].

Для обучения искусственной нейронной сети использовались две модели сетевого трафика – атакующая и нормальная.

Результаты экспериментального исследования приведены в следующей таблице:

Таблица 2. **Результаты работы системы обнаружения атак**

Table 2. **Results of Attack Detection System**

№ попытки эксперимента	Длина вектора	Величина обучающей выборки для пакетов	Величина обучающей выборки для окон	Размер окна	Размер сдвига	Результат на тестовой выборке	
						Ошибка 1-го рода	Ошибка 2-го рода
1.	20	5000	20	1500	750	0.1154	0.8386
2.	20	5000	90	1500	150	0.0554	0.5287
3.	20	5000	160	180	90	0.0011	0.1124
4.	20	5000	800	180	18	0	3.4378e-04
5.	20	5000	900	30	15	0.0118	0.0900
6.	20	5000	4000	30	3	8.1827e-04	0.0050
7.	50	30000	120	1500	750	0	0.0471
8.	50	30000	540	1500	150	0	0.0033
9.	50	30000	960	180	90	0	0.1447
10.	50	30000	4800	180	18	0.0449	0.0449
11.	50	30000	5400	30	15	0.0289	0.0232
12.	50	30000	24000	30	3	0.0367	0.0172

В данной таблице ошибка первого рода – это ложное срабатывание, а ошибка второго рода – пропуск цели. Наилучшие результаты данный метод показал на попытках 6, 7 и 8.

Заключение

В результате оценки эффективности метода обнаружения низкоинтенсивных DoS атак были получены низкие показатели ошибок как первого, так и второго рода. Из этого можно сделать вывод о том, что у данного метода низкий уровень ложных срабатываний и достаточно высокий уровень обнаружения атак за счёт низкого числа необнаруженных атак. Все вышесказанное подтверждает эффективность этого метода.

References

[1] Wu Z., Yue M., Li D., Xie K. SEDP-based detection of low-rate DoS attacks. *International Journal of Communication Systems.* 2014;28(11):1772-1788. doi: https://doi.org/10.1002/dac.2783C

[2] Fu Y., Duan X., Wang K., Li B. Low-rate Denial of Service attack detection method based on time-frequency characteristics. *Journal of Cloud Computing*. 2022;11:31. doi: https://doi.org/10.1186/s13677-022-00308-3

[3] Liu L., Wang H., Wu Z., Yue M. The detection method of low-rate DoS attack based on multi-feature fusion. *Digital Communications and Networks*. 2020;6(4):504-513. doi: https://doi.org/10.1016/j.dcan.2020.04.002

[4] Alashhab A.A., Zahid M.S.M., Azim M.A., Daha M.Y., Isyaku B., Ali S. A Survey of Low Rate DDoS Detection Techniques Based on Machine Learning in Software-Defined Networks. *Symmetry*. 2022;14(8):1563. doi: https://doi.org/10.3390/sym14081563

[5] Zhan S., Tang D., Man J., Dai R., Wang X. Low-Rate DoS Attacks Detection Based on MAF-ADM. *Sensors*. 2020;20(1):189. doi: https://doi.org/10.3390/s20010189

[6] Zhou L., Liao M., Yuan C., Zhang H. Low-Rate DDoS Attack Detection Using Expectation of Packet Size. *Security and Communication Networks*. 2017;2017:3691629. doi: https://doi.org/10.1155/2017/3691629

[7] Cheng J., Yin J., Wu C., Zhang B., Liu Y. DDoS Attack Detection Method Based on Linear Prediction Model. In: Huang D.S., Jo K.H., Lee H.H., Kang H.J., Bevilacqua V. (Eds.) Emerging Intelligent Computing Technology and Applications. ICIC 2009. Lecture Notes in Computer Science. Vol. 5754. Berlin, Heidelberg: Springer; 2009. p. 1004-1013. doi: https://doi.org/10.1007/978-3-642-04070-2_106

[8] Shevtekar A., Ansari N. A Proactive Test Based Differentiation Technique to Mitigate Low Rate DoS Attacks. In: 2007 16th International Conference on Computer Communications and Networks. Honolulu, HI, USA: IEEE Computer Society; 2007. p. 639-644. doi: https://doi.org/10.1109/ICCCN.2007.4317889

[9] van der Maaten L.J.P., Hinton G.E. Visualizing Data using t-SNE. *Journal of Machine Learning Research*. 2008;9(86):2579-2605. Available at: https://www.jmlr.org/papers/v9/vandermaaten08a.html (accessed 11.07.2022).

[10] Velliangiri S., Alagumuthukrishnan S., Iwin Thankumar joseph S. A Review of Dimensionality Reduction Techniques for Efficient Computation. *Procedia Computer Science*. 2019;165:104-111. doi: https://doi.org/10.1016/j.procs.2020.01.079

[11] Mizuta M. Dimension Reduction Methods. In: Gentle J., Härdle W., Mori Y. (Eds.) Handbook of Computational Statistics. Springer Handbooks of Computational Statistics. Berlin, Heidelberg: Springer; 2012. p. 619-644. doi: https://doi.org/10.1007/978-3-642-21551-3_22

[12] Awad M., Khanna R. Machine Learning. In: Efficient Learning Machines. Berkeley, CA: Apress; 2015. p. 1-18. doi: https://doi.org/10.1007/978-1-4302-5990-9_1

[13] Zhang N., Jaafar F., Malik Y. Low-Rate DoS Attack Detection Using PSD Based Entropy and Machine Learning. In: 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). Paris, France: IEEE Computer Society; 2019. p. 59-62. doi: https://doi.org/10.1109/CSCloud/EdgeCom.2019.00020

[14] Tang D., Dai R., Tang L., Li X. Low-rate DoS attack detection based on two-step cluster analysis and UTR analysis. *Human-centric Computing and Information Sciences*. 2020;10(1):6. doi: https://doi.org/10.1186/s13673-020-0210-9

[15] Prakash A., Satish M., Sri Sai Bhargav T., Bhalaji N. Detection and Mitigation of Denial of Service Attacks Using Stratified Architecture. *Procedia Computer Science*. 2016;87:275-280. doi: https://doi.org/10.1016/j.procs.2016.05.161

[16] Brugger D., Bogdan M., Rosenstiel W. Automatic Cluster Detection in Kohonen's SOM. *IEEE Transactions on Neural Networks*. 2008;19(3):442-459. doi: https://doi.org/10.1109/TNN.2007.909556

[17] Jun J.-H., Ahn C.-W., Kim S.-H. DDoS attack detection by using packet sampling and flow features. In: Proceedings of the 29th Annual ACM Symposium on Applied Computing (SAC '14). New York, NY, USA: Association for Computing Machinery; 2014. p. 711-712. doi: https://doi.org/10.1145/2554850.2555109

[18] Saied A., Overill R.E., Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing*. 2016;172:385-393. doi: https://doi.org/10.1016/j.neucom.2015.04.101

[19] Özçelik I., Brooks R.R. Deceiving entropy based DoS detection. *Computers & Security*. 2015;48:234-245. doi: https://doi.org/10.1016/j.cose.2014.10.013

[20] Alzahrani R.J., Alzahrani A. Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic. *Electronics*. 2021;10(23):2919. doi: https://doi.org/10.3390/electronics10232919

[21] Alexis Fidele K., Suryono, Amien Syafei W. Denial of Service (DoS) attack identification and analyse using sniffing technique in the network environment. *E3S Web of Conferences*. 2020;2020:15003. doi: https://doi.org/10.1051/e3sconf/202020215003

[22] Rios V.D.M., Inácio P.R.M., Magoni D., Freire M.M. Detection and Mitigation of Low-Rate Denial-of-Service Attacks: A Survey. *IEEE Access*. 2022;10:76648-76668. doi: https://doi.org/10.1109/ACCESS.2022.3191430

[23] Agrawal N., Tapaswi S. Low rate cloud DDoS attack defense method based on power spectral density analysis. *Information Processing Letters*. 2018;138:44-50. doi: https://doi.org/10.1016/j.ipl.2018.06.001

[24] Mittal M., Kumar K., Behal S. Deep learning approaches for detecting DDoS attacks: a systematic review. *Soft Computing*. 2022. doi: https://doi.org/10.1007/s00500-021-06608-1

[25] Usha G., Narang M., Kumar A. Detection and Classification of Distributed DoS Attacks Using Machine Learning. In: Smys S., Palanisamy R., Rocha Á., Beligiannis G.N. (Eds.) Computer Networks and Inventive Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies. Vol. 58. Singapore: Springer; 2021. p. 985-1000. doi: https://doi.org/10.1007/978-981-15-9647-6_78

Поступила 11.07.2022; одобрена после рецензирования 18.09.2022; принята к публикации 06.11.2022.
Submitted 11.07.2022; approved after reviewing 18.09.2022; accepted for publication 06.11.2022.

Об авторах:

Турашев Артём Сергеевич, студент факультета вычислительной математики и кибернетики, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), **ORCID: https://orcid.org/0000-0001-8391-4948,** turashev.artem@mail.ru

Сухомлин Владимир Александрович, заведующий лабораторией открытых информационных технологий факультета вычислительной математики и кибернетики, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1); ведущий научный сотрудник Института проблем информатики Российской академии наук, ФГУ «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (119333, Российская Федерация, г. Москва, ул. Вавилова, д. 44-2), доктор технических наук, профессор, **ORCID: https://orcid.org/0000-0001-9468-7138**, sukhomlin@mail.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the authors:

Artem S. Turashev, student of the Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), **ORCID: https://orcid.org/0000-0001-8391-4948,** turashev.artem@mail.ru

Vladimir A. Sukhomlin, Head of the Open Information Technologies Lab, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation); Leading Researcher of the Institute of Informatics Problems of the Russian Academy of Sciences, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences (44 Vavilov St., building 2, Moscow 119333, Russian Federation), Dr. Sci. (Tech.), Professor, **ORCID: https://orcid.org/0000-0001-9468-7138**, sukhomlin@mail.ru

All authors have read and approved the final manuscript.