УДК 656.6; 656.61;656.62/.66
DOI: 10.17586/0021-3454-2021-64-6-452-458

ОЦЕНКА ФУНКЦИОНАЛЬНОГО СОСТОЯНИЯ ОБЪЕКТА СЕТЕВОЙ ИНФРАСТРУКТУРЫ ПРИ ПОМОЩИ НЕЙРОСЕТЕВОГО ПОДХОДА

И. А. Сикарев[1], М. Е. Сухопаров[1], О. В. Петриева[2]

[1]*Российский государственный гидрометеорологический университет, 192007, Санкт-Петербург, Россия*
E-mail: sikarev@yandex.ru

[2]*Санкт-Петербургский университет ГПС МЧС России, 196105, Санкт-Петербург, Россия*

Рассмотрены вопросы оценки функционального состояния объектов сетевой инфраструктуры, обоснована необходимость использования альтернативных методов оценки. Описаны побочные каналы, с использованием которых возможно отслеживать состояния отдельных объектов. Проведен эксперимент, в котором с помощью двух датчиков осуществлялось считывание статистической информации о различных режимах работы устройства сетевой архитектуры. Полученные данные обрабатывались двуслойной нейронной сетью прямого распространения с сигмоидальной передаточной функцией в скрытых слоях. Полученную модель поведения объекта сетевой инфраструктуры можно использовать в качестве дополнительного элемента для определения функционального состояния.

Ключевые слова: *сенсор, вычислительная сеть, несанкционированный доступ, сигнал, графовая модель, нейронная сеть, интеграция*

Введение. Повсеместное использование сенсоров и датчиков, автоматизация производственного процесса, массовая интеграция систем „умных“ городов и пространств, минимизация стоимости и размеров вычислительных узлов — основные направления развития технологий, базирующихся на концепции интернета вещей (IoT).

Отсутствие контролируемой зоны, относительная доступность, связанная с применением беспроводных сетевых технологий, важность для критической инфраструктуры различных систем технологических процессов делают IoT-устройства привлекательными целями возможных деструктивных воздействий, что, в свою очередь, может приводить к необратимым последствиям [1, 2].

Ежегодные отчеты, например от компании Cisco, показывают тенденцию роста количества атак на сетевую архитектуру производственных систем (приводятся примеры успешных атак на системы управления процессами критических информационных структур, таких как электростанции, центры управления городским водоснабжением, промышленные предприятия и т.д.), IoT-устройства (с ростом популярности технологии расширяются и IoT-ботнеты). Убытки от потери работоспособности сетей и телекоммуникаций колоссальны. Анализ состояния элементов систем, обнаружение деструктивных воздействий в ходе эксплуатации необходимы для обеспечения работоспособности инфраструктуры устройств и узлов вычислительных сетей (ВС).

Увеличение частоты использования вредоносного программного обеспечения не позволяет говорить об отсутствии компрометации даже на уровне прошивки контроллеров, а не только встроенных средств защиты или программного кода приложений, используемых в качестве базовых элементов построения типовых систем. Вследствие этого побочные каналы могут выступать альтернативным источником информации для оценки функционального со-

стояния элементов сетевой инфраструктуры. В качестве таких источников могут выступать: акустический, временной каналы, электромагнитное излучение и т.д. [3, 4].

Полученные таким образом данные можно использовать для мониторинга функционального состояния узлов и устройств сетевой инфраструктуры.

Постановка задачи. Повсеместное использование автономных вычислительных устройств обусловливает необходимость решения проблемных вопросов [5], связанных с:

— обнаружением несанкционированного доступа на программном уровне;

— выявлением аномалий в технологических циклах функционирования и их анализом,

— обнаружением деструктивного информационного воздействия на программы и алгоритмы,

— обнаружением не декларированных возможностей.

Невозможность гарантированной защиты от несанкционированного перепрограммирования, внедрения вредоносного кода вызывает необходимость разработки внешних систем контроля, в основе которых могут быть методы анализа поведенческих характеристик, идентифицируемых по акустическим, электромагнитным, механическим побочным каналам. В рассматриваемом случае состояния C определяются сигналами F, представляющими собой набор значений амплитуд $A_1, A_2..., A_n$.

Синхронизированная по временным дискретам последовательность значений амплитуд $\{\{a_1(t_1), a_1(t_2), \dots a_1(t_m)\}, \{a_2(t_1), a_2(t_2), \dots a_2(t_m)\}, \{a_n(t_1), a_n(t_2), \dots a_n(t_m)\}$ будет обусловливать значения показателей, получаемых в результате выполнения определенного действия объектом сетевой инфраструктуры [3, 6].

Матрицы вида:

$$F(t) = \begin{vmatrix} a_1(0) & a_1(1) & \dots & a_1(m) \\ a_2(0) & a_2(1) & \dots & a_2(m) \\ \dots & \dots & \dots & \dots \\ a_n(0) & a_n(1) & \dots & a_n(m) \end{vmatrix} \quad (1)$$

позволяют свести решение к решению задачи классификации, где множество классов принимает значения $C = \{C_0, C_1\}$, C_0 — безопасное состояние, при котором совершается идентифицируемое действие, и C_1 — небезопасное состояние, при котором действие в данный момент отличается от вызванного управляющей командой.

Предлагаемый подход. В работах [7—10] рассматривались возможности использования акустического, электромагнитного излучения микросхем, принципы анализа состояний объектов, применяемые при оценивании состояния.

В качестве дополнения к побочному каналу можно использовать поведенческие характеристики объектов, которые позволяют обнаруживать аномалии, связанные с задержкой выполнения команд, появления фоновых шумов и вибраций.

Для анализа используется граф переходов, который отражает состояния объекта сетевой инфраструктуры. Управляющие команды, среда, где функционируют устройства, вызывают определенные внешние и внутренние изменения, фиксируемые на основе характеристик побочных каналов.

Последовательность переходов состояний определяется моделью поведения сетевого устройства. Например, элемент сетевой инфраструктуры Индустрии 4.0, выполняющий обработку и анализ, может характеризоваться только: S_0 — состоянием ожидания, S_1 — состоянием обработки команд.

Графовая модель описывает поведение объекта при возникновении различных событий, где вероятности переменной класса C:

$$P\left(C \middle| a_1, a_2, ..., a_n\right). \quad (2)$$

Один из подходов к *идентификации* состояния может базироваться на использовании нейросетей. Многократное повторение команд позволяет получить временные ряды, отражающие текущее состояние устройства. Определив длину временного ряда и синхронизировав полученные значения, возможно сформировать обучающую выборку.

Таким образом, подавая на вход временные ряды, отражающие характеристики амплитуды, частоты сигналов, получаемых от побочных каналов при выполнении действий, возможно классифицировать состояние объекта.

С помощью различных датчиков, регистрирующих временные ряды при выполнении устройством соответствующих команд, можно обеспечить внешнюю систему контроля.

В эксперименте использован электромагнитный канал. Для определения поведения объекта формируется модель состояний, где выделяется ряд S_0—S_6 (прием данных, передача данных, обработка данных, ожидание передачи данных, формирование ответа, ожидание приема данных, выполнение служебных команд).

Каждое состояние элемента инфраструктуры Индустрии 4.0 должно длиться определенное число дискрет времени. Это число задается временем реакции на полученную команду, промежуток времени между выполнением двух последующих команд связан с вычислительными процессами на устройстве. Такое допущение позволяет производить анализ на основе дискретных состояний и применять для классификации математический аппарат на основе нейросетевого подхода.

Нейронная сеть обучается путем многократного повторения действий по получению спектральной информации в состояниях S_0—S_6. В каждом состоянии накапливаются спектральные данные датчиков, на основе которых происходит обучение сети. Класс текущего состояния C_i задается множеством характеристик, определяющих наибольшую вероятность:

$$C = \arg\max_i p_i .$$

В работах [3, 5, 11] показано, что такой подход обеспечивает результаты, позволяющие реализовать классификацию с точностью на уровне 0,8. В то же время применение модели состояний дает возможность определить, из какого состояния в какое может быть выполнен переход системы. Например, из состояния S_3 в последующий дискретный момент времени объект может оказаться в S_1 или S_0, а из состояния S_1 — перейти в S_0, S_3, S_4 и т.д. Таким образом, сегментация позволяет не рассматривать все возможные состояния, а осуществлять классификацию над ограниченным набором, а следовательно, с учетом появления нестандартных значений, исключая недопустимые переходы состояний.

Эксперимент. Возможности приведенного подхода экспериментально проверены, схема эксперимента приведена на рис. 1.

Электромагнитный канал выбран в качестве источника получения значений поведенческих характеристик. Датчики для съема сигнала находились на объекте сетевой инфраструктуры в зоне проведения эксперимента. В ходе эксперимента продолжительность команд изменялась в диапазоне 5—15 с. Полученные данные были оцифрованы. Для корректного анализа преимуществ и недостатков метода условия эксперимента выбраны в точности совпадающими с описанными в [12—14].

При дискретизации каждого непрерывного по времени сигнала, содержащего значения амплитуд по двум каналам, из него взято 7000 отсчетов. Полученные значения обработаны при помощи двуслойных нейронных сетей прямого распространения с сигмоидальной передаточной функцией.

Количество входных нейронов равно количеству используемых датчиков, измеряющих амплитуды сигнала, скрытых нейронов — 300, число выходных нейронов соответствует числу исследуемых состояний автономного объекта — 6; выход нейросети — значения вероятностей отношения текущего состояния к конкретному классу.

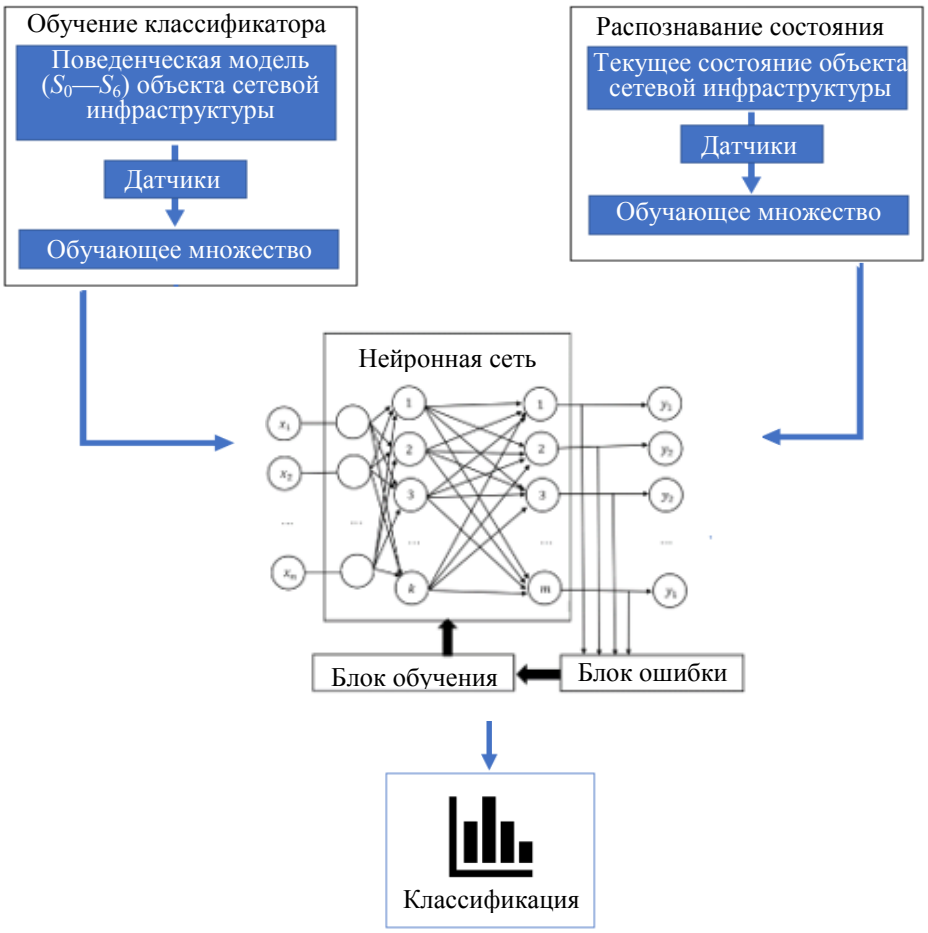

Рис. 1

Классификация выполнялась по шести состояниям. Для формирования обучающей выборки использовалось 70 % значений, 15 % значений использовались в качестве тестового и еще 15 % — в качестве проверочного набора.

На рис. 2—4 представлены результаты классификации (рис. 2 — сегментируемые классы S_0, S_1, S_3, общая точность 0,89; рис. 3 — S_0, S_1, S_3, S_4, общая точность 0,84; рис. 4 — S_0, S_2, S_5, S_6, общая точность 0,81; n — расчетный класс).

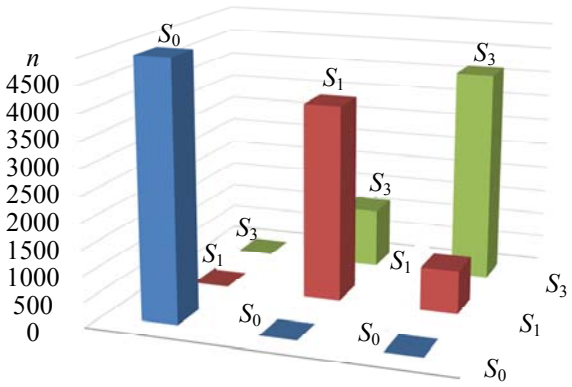

Рис. 2

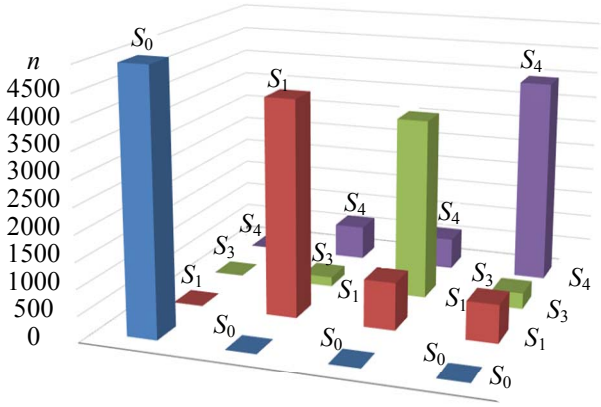

Рис. 3

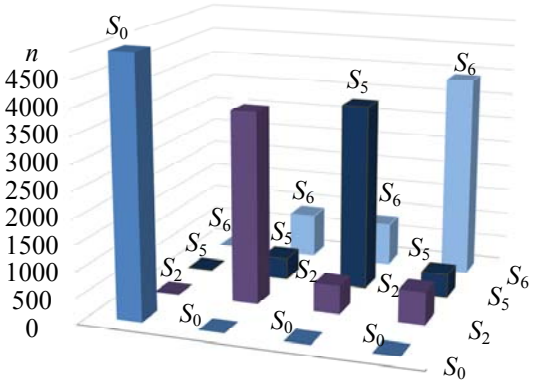

Рис. 4

Из рис. 2—4 видно, что, используя два датчика (в отличие от одного в [12—14]), система мониторинга позволяет получить вероятность выявления различных состояний свыше 0,8.

Заключение. Анализ объекта как черного ящика, отсутствие постоянного контроля над ним, требование доступа к объекту с использованием открытых сетей обусловливают необходимость идентификации внутренних и внешних процессов. Применение внутренних средств мониторинга не позволяет в полной мере гарантировать отсутствие компрометации вычислительного устройства на уровне программного кода, поэтому все большую актуальность приобретают средства, использующие независимые каналы, основанные на принципах измерения физических параметров, и поиска корреляции их изменений с потреблением энергии, временем вычислений, электромагнитной индукцией и т.д.

Рассмотренный подход может быть полезен, когда процессы, протекающие во время функционирования устройства, недоступны наблюдателю.

Сегментация обеспечивает повышение точности определения функционального состояния устройств и узлов сетевой инфраструктуры. Предложенная модель с использованием сегментации позволила с вероятностью более 0,8 выявить различия в состояниях информационной безопасности автономного объекта.

СПИСОК ЛИТЕРАТУРЫ

1. *Heller K. A., Svore K. M., Keromytis A. D., Stolfo S. J.* One class support vector machines for detecting anomalous windows registry accesses // Proc. Workshop Data Mining for Computer Security. 2003. Vol. 9. https://www.researchgate.net/publication/2883103_One_Class_Support_Vector_Machines_for_Detecting_Anomalous_Windows_Registry_Accesses.

2. *Сухопаров М. Е., Семенов В. В., Лебедев И. С.* Модель поведения для классификации состояния информационной безопасности автономного объекта // Проблемы информационной безопасности. Компьютерные системы. 2019. № 4. С. 26—34.

3. *Hayashi Y. I., Homma N., Watanabe T., Price W. O., Radasky W. A.* Introduction to the Special Section on Electromagnetic Information Security // Proc. IEEE Transactions on Electromagnetic Compatibility. June 2013. Vol. 55, N 3. P. 539—546.

4. *Han Y., Christoudis I., Diamantaras K. I., Zonouz S., Petropulu A.* Side-Channel-Based Code-Execution Monitoring Systems: A Survey // IEEE Signal Processing Magazine. 2019. Vol. 36, N 2. P. 22—35.

5. *Lebedev I. S., Semenov V. V., Sukhoparov M. E., Salakhutdinova K. I.* Application of an autonomous object behavior model to classify the cybersecurity state // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 2019. P. 104—112.

6. *Malafeyev O. A., Redinskikh N. D., Nemnyugin S. A., Kolesin I. D., Zaitseva I. V.* The optimization problem of preventive equipment repair planning // AIP Conf. Proc. Intern. Conf. of Numerical Analysis and Applied Mathematics. ICNAAM 2017. 2018. P. 1000135.

7. *Han Y., Etigowni S., Liu H., Zonouz S., Petropulu A.* Watch Me, but Don't Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations // Proc. ACM Conf. on Computer and Communications Security. 2017. P. 1095—1108.

8. *Genkin D., Shamir A., Tromer E.* Acoustic Cryptanalysis // J. of Cryptology. 2017. Vol. 30, N 2. P. 392—443.

9. *Kutuzov O. I., Tatarnikova T. M.* On the acceleration of simulation modeling // Proc. of 2019 22nd Intern. Conf. on Soft Computing and Measurements, SCM 2019. 2019. P. 45—47.

10. *Malafeyev O., Lakhina J., Redinskikh N., Smirnova T., Smirnov N., Zaitseva I.* A mathematical model of production facilities location // Journal of Physics: Conference Series. 2019. P. 012090.

11. *Татарникова Т. М.* Аналитико-статистическая модель оценки живучести сетей с топологией MESH // Информационно-управляющие системы. 2017. № 1(86). С. 17—22.

12. *Семенов В. В., Лебедев И. С.* Обработка сигнальной информации в задачах мониторинга информационной безопасности автономных объектов беспилотных систем // Науч.-техн. вестн. информационных технологий, механики и оптики. 2019. Т. 19, № 3. С. 105—111.

13. *Sikarev I. A., Sakharov V. V., Garanin A. V.* On Improving the Reliability and Information Security of Information Transmission Systems in Communication Channels of an Unmanned Vessel // Automatic Control and Computer Sciences. 2020. Vol. 54, N 8. P. 894—897.

14. *Sikarev I. A., Chistyakov G. B., Garanin A. V., Moskvin D. A.* Algorithms for Enhancing Information Security in the Processing of Navigation Data of Unmanned Vessels of the Technical Fleet of the Inland Waterways of the Russian Federation // Automatic Control and Computer Sciences. 2020. Vol. 54, N 8. P. 962—965.

Сведения об авторах

Игорь Александрович Сикарев — д-р техн. наук, профессор; РГГМУ, кафедра морских информационных систем; заведующий кафедрой; E-mail: sikarev@yandex.ru

Михаил Евгеньевич Сухопаров — канд. техн. наук; РГГМУ, кафедра морских информационных систем; доцент; E-mail: sukhoparovm@gmail.com

Оксана Владимировна Петриева — канд. техн. наук, доцент; Санкт-Петербургский университет ГПС МЧС России, кафедра высшей математики и системного моделирования сложных процессов; E-mail: oksenj_pet@mail.ru

Поступила в редакцию
28.01.2021 г.

Ссылка для цитирования: *Сикарев И. А., Сухопаров М. Е., Петриева О. В.* Оценка функционального состояния объекта сетевой инфраструктуры при помощи нейросетевого подхода // Изв. вузов. Приборостроение. 2021. Т. 64, № 6. С. 452—458.

ASSESSMENT OF THE FUNCTIONAL STATE OF A NETWORK INFRASTRUCTURE OBJECT USING A NEURAL NETWORK APPROACH

I. A. Sikarev[1], M. E. Sukhoparov[1], O. V. Petrieva[2]

[1]*Russian State Hydrometeorological University, 192007, St. Petersburg, Russia*
E-mail: sikarev@yandex.ru

[2]*St. Petersburg University of state fire service of EMERCOM of Russia, 196105, St. Petersburg, Russia*

The issues of assessing the functional state of network infrastructure objects are considered, and the need for using alternative assessment methods is justified. Side channels are described, with the use of which it becomes possible to monitor the states of individual objects. The experiment conducted in the framework of the study is described. With the help of two sensors, statistical information about the various operating modes of the network architecture device was read. The obtained data were processed using two-layer direct propagation neural networks with a sigmoidal transfer function in hidden layers. The resulting behavior model of the network infrastructure object can be used as an additional element for determining the functional state.

Keywords: sensor, computer network, unauthorized access, signal, graph model, neural network, integration

REFERENCES

1. Heller K A., Svore K.M., Keromytis A.D., Stolfo S.J. *Proc. Workshop Data Mining for Computer Security*, 2003, vol. 9, https://www.researchgate.net/publication/ 2883103_One_Class_Support_ Vector_Machines_for_Detecting_Anomalous_Windows_Registry_Accesses.
2. Sukhoparov M.E., Semenov V.V., Lebedev I.S. *Problems of Information Security. Computer Systems*, 2019, no. 4, pp. 26–34. (in Russ.)
3. Hayashi Y.I., Homma N., Watanabe T., Price W.O., Radasky W.A. *Proc. IEEE Transactions on Electromagnetic Compatibility*, June 2013, no. 3(55), pp. 539–546.
4. Han Y., Christoudis I., Diamantaras K.I., Zonouz S., Petropulu A. *IEEE Signal Processing Magazine*, 2019, no. 2(36), pp. 22–35.
5. Lebedev I.S., Semenov V.V., Sukhoparov M.E., Salakhutdinova K.I. *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, 2019, pp. 104–112.
6. Malafeyev O.A., Redinskikh N.D., Nemnyugin S.A., Kolesin I.D., Zaitseva I.V. *AIP Conference Proceedings. International Conference of Numerical Analysis and Applied Mathematics*, ICNAAM 2017, 2018, pp. 1000135.
7. Han Y., Etigowni S., Liu H., Zonouz S., Petropulu A. *Proceedings of the ACM Conference on Computer and Communications Security*, 2017, pp. 1095–1108.
8. Genkin D., Shamir A., Tromer E. *Journal of Cryptology*, 2017, no. 2(30), pp. 392–443.
9. Kutuzov O.I., Tatarnikova T.M. *Proceedings of 2019 22nd International Conference on Soft Computing and Measurements*, SCM 2019, 2019, pp. 45–47.
10. Malafeyev O., Lakhina J., Redinskikh N., Smirnova T., Smirnov N., Zaitseva I. *Journal of Physics: Conference Series*, 2019, pp. 012090.
11. Tatarnikova T.M. *Information and Control Systems*, 2017, no. 1(86), pp. 17–22. (in Russ.)
12. 8 Semenov V.V., Lebedev I.S. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2019, no. 3(19), pp. 105–111. (in Russ.)
13. Sikarev I.A., Sakharov V.V., Garanin A.V. *Automatic Control and Computer Sciences*, 2020, no. 8(54), pp. 894–897.
14. Sikarev I.A., Chistyakov G.B., Garanin A.V., Moskvin D.A. *Automatic Control and Computer Sciences*, 2020, no. 8(54), pp. 962–965.

Data on authors

Igor A. Sikarev	—	Dr. Sci., Professor; Russian State Hydrometeorological University Department of Marine Information Systems; Head of the Department; E-mail: sikarev@yandex.ru
Michael E. Sukhoparov	—	PhD; Russian State Hydrometeorological University, Department of Marine Information Systems; Associate Professor; E-mail: sukhoparovm@gmail.com
Oksana V. Petrieva	—	PhD, Associate Professor; St. Petersburg University of State Fire Service of EMERCOM of Russia, Department of Higher Mathematics and System Modeling of Complex Processes; E-mail: oksenj_pet@mail.ru

For citation: Sikarev I. A., Sukhoparov M. E., Petrieva O. V. Assessment of the functional state of a network infrastructure object using a neural network approach. *Journal of Instrument Engineering*. 2021. Vol. 64, N 6. P. 452—458 (in Russian).

DOI: 10.17586/0021-3454-2021-64-6-452-458