УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
сентябрь–октябрь 2020 Том 20 № 5 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
September–October 2020 Vol. 20 No 5 ISSN 2226-1494 http://ntv.ifmo.ru/en/
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

УДК 004.021 doi: 10.17586/2226-1494-2020-20-5-770-772

ВЫЯВЛЕНИЕ РИСКОВ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА ОСНОВЕ АНАЛИЗА ЦИФРОВЫХ СИГНАЛОВ

В.В. Семенов[a,b], С.А. Арустамов[b]

[a] Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН), Санкт-Петербург, 199178, Российская Федерация
[b] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: semenov@itmo.ru

Информация о статье
Поступила в редакцию 23.07.20, принята к печати 30.08.20
Язык статьи — русский

Ссылка для цитирования: Семенов В.В., Арустамов С.А. Выявление рисков нарушений информационной безопасности киберфизических систем на основе анализа цифровых сигналов // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 5. С. 770–772. doi: 10.17586/2226-1494-2020-20-5-770-772

Аннотация

Предмет исследования. В работе предложен подход к анализу цифровых последовательностей сигналов, характеризующих функционирование киберфизических систем. Предлагаемое решение сочетает в себе совокупность методов машинного обучения при анализе разнородных внешних данных цифровых сигналов, поступающих от различных датчиков системы. **Метод.** Для анализа цифровых сигналов исследованы методы на основе искусственных нейронных сетей и алгоритма *k*-ближайших соседей. **Основные результаты.** Проверка предлагаемого подхода произведена с использованием полученных в эксперименте сигналов цифрового трехосевого акселерометра, расположенного на прототипе беспилотного транспортного средства. Обработка цифровых сигналов исследуемыми методами произведена в среде MATLAB R2020a. При проведении сравнения точности исследованных методов алгоритм *k*-ближайших соседей достиг значения 96,1 %, в то время как искусственные нейронные сети показали результат 95,0 %. **Практическая значимость.** Предложенный подход позволяет с приемлемой точностью обнаруживать риски нарушений информационной безопасности киберфизических систем и может использоваться в системах мониторинга состояния объектов.

Ключевые слова
информационная безопасность, киберфизические системы, выявление рисков, анализ сигналов, системы мониторинга

Благодарности
Статья подготовлена при финансовой поддержке Министерства науки и высшего образования Российской Федерации по соглашению 075-15-2019-1707 от 22.11.2019 (идентификатор RFMEFI60519X0189, внутренний номер 05.605.21.0189)

doi: 10.17586/2226-1494-2020-20-5-770-772

RISK IDENTIFICATION OF SECURITY INFORMATION VIOLATIONS IN CYBER-PHYSICAL SYSTEMS BASED ON ANALYSIS OF DIGITAL SIGNALS

V.V. Semenov[a,b], S.A. Arustamov[b]

[a] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), Saint Petersburg, 199178, Russian Federation
[b] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: semenov@itmo.ru

Article info
Received 23.07.20, accepted 30.08.20
Article in Russian

For citation: Semenov V.V., Arustamov S.A. Risk identification of security information violations in cyber-physical systems based on analysis of digital signals. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2020, vol. 20, no. 5, pp. 770–772 (in Russian). doi: 10.17586/2226-1494-2020-20-5-770-772

Abstract

Subject of Research. The paper presents an approach to the analysis of digital signal sequences related to cyber-physical systems functioning. The proposed solution combines a set of machine learning methods for analyzing heterogeneous external data of digital signals coming from various system sensors. **Method.** The methods based on artificial neural networks and the *k*-nearest neighbors algorithm were studied for the analysis of digital signals. **Main Results.** The

proposed approach has been tested using the signals received from a digital three-axis accelerometer located on an unmanned vehicle prototype. The processing of digital signals by the methods under study has been carried out in the MATLAB R2020a environment. The accuracy of the researched methods has been compared and, as a result, the *k*-nearest neighbors algorithm reached the value of 96.1 %, whereas artificial neural networks showed the result of 95.0 %. **Practical Relevance.** The proposed approach makes it possible to detect the risks of information security violations of the cyber-physical systems with acceptable accuracy and can be used in systems for the state monitoring of objects.

Keywords
information security, cyber-physical systems, risk identification, signal analysis, monitoring systems

Acknowledgements
The paper was prepared with the financial support of the Ministry of Science and Higher Education of the Russian Federation under the agreement No. 075-15-2019-1707 dated from 22.11.2019 (identifier RFMEFI60519X0189, internal number 05.605.21.0189).

Киберфизические системы (КФС), являясь основой для реализаций множества современных инновационных решений, существенно уязвимы с точки зрения успешных информационных атак, приводящих к критическим сбоям или аномальному функционированию. Успешная реализация атак КФС, тесно интегрированных в различные отрасли деятельности, способна привести не только к финансовому ущербу, но и к серьезным техногенным, экологическим катастрофам и человеческим жертвам.

На сегодняшний день имеется множество работ отечественных и зарубежных исследователей, посвященных разработке методов и систем обнаружения нарушений информационной безопасности (ИБ) КФС [1–4]. Преимущественно исследования сконцентрированы на поиске аномалий в поведении системы, которые могут быть вызваны атаками злоумышленников или внедрением вредоносного программного обеспечения в КФС. Большинство работ современных исследователей сосредоточено на анализе либо физической [5, 6], либо информационной [7] составляющих КФС. Так, авторы работы [8] предлагают основанный на машинном обучении подход обнаружения аномальных данных от датчиков в КФС водоснабжения. Точность на построенном наборе данных при использовании алгоритма *k*-ближайших соседей (*k*-nearest neighbors, *k*-NN) составляет 83–87 % и зависит от параметра модели *k*.

Исходя из анализа современных исследований и технических решений, можно сделать вывод о том, что в настоящее время в мире отсутствуют комплексные подходы, направленные на выявление рисков нарушений ИБ систем, реализующих информационные и физические процессы одновременно.

В исследуемой задаче формируется n временных рядов $X = \{\{x_1(t_1), x_1(t_2), \ldots, x_1(t_m)\}, \{x_2(t_1), x_2(t_2), \ldots, x_2(t_m)\}, \{x_n(t_1), x_n(t_2), \ldots, x_n(t_m)\}\}$, представляющих собой синхронизированные по времени множества значений сигналов с различных датчиков КФС. Требуется при заданном количестве доступных датчиков n и минимальном времени накопления статистической информации ($t_m \to \min$) выявить риски нарушений ИБ системы с достаточной точностью.

В рамках поставленной задачи авторы исследовали эффективность двух различных методов машинного обучения для анализа цифровых сигналов, характеризующих функционирование КФС с целью выявления рисков нарушений ИБ КФС. Для проверки предлагаемого подхода выполнен эксперимент с прототипом беспилотного транспортного средства (БТС) в качестве исследуемой КФС. В эксперименте исследованы шесть различных состояний, три из которых были штатными, а в остальных трех при помощи подмены управляющего сигнала моделировались риски нарушений ИБ. Полученные цифровые сигналы обрабатывались в среде MATLAB R2020a с помощью алгоритма *k*-NN при разных значениях параметра k и двухслойных искусственных нейронных сетях (ИНС) прямого распространения с сигмоидальной передаточной функцией в скрытых слоях. Количество скрытых нейронов ИНС — 300.

Признаковое пространство разделено на два класса C_0 и C_1. Класс C_0 включает в себя безопасные состояния, и класс C_1, в исследуемых состояниях которого моделируются различные риски нарушений ИБ. Наилучшая точность метода классификации на основе алгоритма *k*-NN при использовании полученных экспериментальных данных наблюдается при $k = 3$ и уменьшается с увеличением k. По всей видимости, это связано с тем, что при увеличении k в связи с возрастанием вычислительной сложности алгоритма, некоторые

Таблица. Матрица несоответствий, полученная в результате классификации состояний прототипа беспилотного транспортного средства

Классификатор		Истинный класс			
		k-NN ($k = 3$)		ИНС	
		C_1	C_0	C_1	C_0
Прогнозируемый класс	C_1	580 48,3 %	27 2,2 %	574 47,8 %	33 2,8 %
	C_0	20 1,7 %	573 47,8 %	26 2,2 %	567 47,2 %

особенности процессов функционирования КФС не учитываются. Результаты классификации приведены в таблице. Верхняя цифра в каждой ячейке показывает число состояний, отнесенных классификатором к тому или иному классу, а нижняя — процент от общего числа исследуемых состояний. В залитых ячейках представлены результаты, в которых класс определен верно, в незалитых – ошибки первого и второго рода.

Таким образом, за счет представления процессов КФС в виде последовательностей значений цифровых сигналов по времени предложенные методы анализа являются универсальными и инвариантными к типам деструктивных воздействий. Описанные методы также позволяют проводить мультиклассификацию и не требуют обязательной настройки или адаптации измерительных устройств к обнаружению конкретных видов атак. При использовании алгоритма *k*-NN ошибки первого рода — 2,2 %, ошибки второго рода — 1,7 %, у метода на основе ИНС: 2,8 % и 2,2 % соответственно.

Точность предложенных методов на основе результатов серии экспериментов составила 96,1 % с применением алгоритма *k*-NN и 95,0 % с применением ИНС, что является достаточным для решения задачи выявления рисков нарушений ИБ для прототипа БТС и превосходит результаты, опубликованные в [8]. К недостаткам подхода можно отнести сильное влияние посторонних шумов, не связанных с процессами КФС. В случае апостериорного расследования инцидента ИБ рекомендуется использовать метод на основе алгоритма *k*-NN, поскольку вычислительная сложность *k*-NN увеличивается с ростом набора обучающих данных, а в случае мониторинга системы в реальном времени — метод на основе ИНС.

Литература

1. Зегжда Д.П., Павленко Е.Ю. Гомеостатическая стратегия безопасности киберфизических систем // Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 9–23.
2. Викснин И.И., Комаров И.И., Масленников О.С., Мурадов А.Р., Пантюхин И.С., Юрьева Р.А. Подход к обнаружению новых кибератак на киберфизические системы на основании метода обнаружения аномалий // Автоматизация в промышленности. 2018. № 2. С. 58–62.
3. Peng Y., Lu T., Liu J., Gao Y., Guo X., Xie F. Cyber-physical system risk assessment // Proc. 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2013). Beijing, China. 2013. P. 442–447. doi: 10.1109/IIH-MSP.2013.116
4. Semenov V.V., Lebedev I.S., Sukhoparov M.E., Salakhutdinova K.I. Application of an autonomous object behavior model to classify the cybersecurity state // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2019. V. 11660. P. 104–112. doi: 10.1007/978-3-030-30859-9_9
5. Jones A., Kong Z., Belta C. Anomaly detection in cyber-physical systems: A formal methods approach // Proc. 53rd IEEE Annual Conference on Decision and Control (CDC 2014). 2014. P. 848–853. doi: 10.1109/CDC.2014.7039487
6. Семенов В.В., Салахутдинова К.И., Лебедев И.С., Сухопаров М.Е. Выявление аномальных отклонений при функционировании устройств киберфизических систем // Прикладная информатика. 2019. Т. 14. № 6(84). С. 114–122. doi: 10.24411/1993-8314-2019-10053
7. Narang P., Sikdar B. Anomaly detection in diurnal CPS monitoring data using a local density approach // Proc. 24th IEEE International Conference on Network Protocols, (ICNP 2016). 2016. P. 7785323. doi: 10.1109/ICNP.2016.7785323
8. Meleshko A.V., Desnitsky V.A., Kotenko I.V. Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems // IOP Conference Series: Materials Science and Engineering. 2020. V. 709. N 3. P. 033034. doi: 10.1088/1757-899X/709/3/033034

References

1. Zegzhda D.P., Pavlenko E.Y. Homeostatic security of cyber-physical systems. *Information Security Problems. Computer Systems*, 2017, no. 3, pp. 9–23. (in Russian)
2. Viksnin I.I., Komarov I.I., Maslennikov O.S., Muradov A.R., Pantiukhin I.S., Iureva R.A. Anomaly detection method for discovery of new cyber attacks on cyber physical systems. *Automation in Industry*, 2018, no. 2, pp. 58–62. (in Russian)
3. Peng Y., Lu T., Liu J., Gao Y., Guo X., Xie F. Cyber-physical system risk assessment. *Proc. 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2013)*, Beijing, China, 2013, pp. 442–447. doi: 10.1109/IIH-MSP.2013.116
4. Semenov V.V., Lebedev I.S., Sukhoparov M.E., Salakhutdinova K.I. Application of an autonomous object behavior model to classify the cybersecurity state. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11660, pp. 104–112. doi: 10.1007/978-3-030-30859-9_9
5. Jones A., Kong Z., Belta C. Anomaly detection in cyber-physical systems: A formal methods approach. *Proc. 53rd IEEE Annual Conference on Decision and Control (CDC 2014)*, 2014, pp. 848–853. doi: 10.1109/CDC.2014.7039487
6. Semenov V., Salakhutdinova K., Lebedev I., Sukhoparov M. Identification of abnormal functioning during the operation devices of cyber-physical systems. *Journal of Applied Informatics*, 2019, vol. 14, no. 6(84), pp. 114–122. (in Russian). doi: 10.24411/1993-8314-2019-10053
7. Narang P., Sikdar B. Anomaly detection in diurnal CPS monitoring data using a local density approach. *Proc. 24th IEEE International Conference on Network Protocols, (ICNP 2016)*, 2016, pp. 7785323. doi: 10.1109/ICNP.2016.7785323
8. Meleshko A.V., Desnitsky V.A., Kotenko I.V. Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems. *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 709, no. 3, pp. 033034. doi: 10.1088/1757-899X/709/3/033034

Авторы

Семенов Виктор Викторович — младший научный сотрудник, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН), Санкт-Петербург, 199178, Российская Федерация; инженер-исследователь, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 57204123255, ORCID ID: 0000-0002-7216-769X, semenov@itmo.ru

Арустамов Сергей Аркадьевич — доктор технических наук, профессор, профессор, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56695216400, ORCID ID: 0000-0002-7520-8987, saarustamov@itmo.ru

Authors

Viktor V. Semenov — Junior Scientific Researcher, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), Saint Petersburg, 199178, Russian Federation; Research Engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 57204123255, ORCID ID: 0000-0002-7216-769X, semenov@itmo.ru

Sergey A. Arustamov — D.Sc., Full Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56695216400, ORCID ID: 0000-0002-7520-8987, saarustamov@itmo.ru