Идентификация состояния мехатронных элементов «Индустрии 4.0» на основе поведенческих паттернов

Identification of the state of mechatronic elements of Industry 4.0 based on behavioral patterns

Сухопаров / Sukhoparov M.
Михаил Евгеньевич
(sukhoparovm@gmail.com)
кандидат технических наук.
Санкт-Петербургский филиал АО «НПК «ТРИСТАН»,
старший научный сотрудник.
г. Санкт-Петербург

Семенов / Semenov V.
Виктор Викторович
(vksemenov@gmail.com)
ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), младший научный сотрудник лаборатории интеллектуальных систем.
г. Санкт-Петербург

Лебедев / Lebedev I.
Илья Сергеевич
(isl_box@mail.ru)
доктор технических наук, профессор.
СПИИРАН,
заведующий лаборатории интеллектуальных систем.
г. Санкт-Петербург

Бойцова / Boitsova E.
Эвелина Павловна
(kiokomiss@gmail.com)
СПИИРАН, аспирант лаборатории интеллектуальных систем.
г. Санкт-Петербург

Ключевые слова: state analysis – анализ состояния; behavioral patterns – поведенческие паттерны; nodes and devices of Industry 4.0. – узлы и устройства «Индустрии 4.0»

Рассмотрены проблемные вопросы состояния мехатронных элементов «Индустрии 4.0». Раскрыты предпосылки, определяющие необходимость использования внешних систем мониторинга. Показан вид и статистические характеристики используемых для анализа поведенческих паттернов. Предлагаемый подход анализа состояния автономного объекта основан на методах кластеризации и позволяет идентифицировать текущее состояние на основе обработки оцифрованных трасс сигналов. Описан эксперимент, направленный на получение статистической информации о различных видах перемещений элемента мехатронного устройства.

The problematic issues of the state of mechatronic elements of Industry 4.0 are considered. The prerequisites that determine the need to use external monitoring systems are disclosed. The type and statistical characteristics of the behavioral patterns used for analysis are shown. The proposed approach to analyzing the state of an autonomous object is based on clustering methods and allows you to identify the current state based on the processing of digital signal paths. An experiment is described aimed at obtaining statistical information about various types of movements of an element of a mechatronic device.

Введение

Развитие технологий, сочетающих в себе сетевые, вычислительные и физические процессы, определяют технологии киберфизических систем «Индустрии 4.0». Смещение акцентов на встраиваемое программное обеспечение, содержащее в себе компоненты искусственного интеллекта, осуществляющие вычисление, сбор и анализ данных, обуславливает необходимость контроля протекающих внутри процессов [1].

Реализация киберфизических систем «Индустрии 4.0» имеет тенденцию, связанную с унификацией компонент, которые могут использоваться в различных устройствах производства, городской инфраструктуры, биомедицинских систем [2].

Доступ к таким устройствам осуществляется как удаленно, так и физически, что значительно расширяет возможности внешних деструктивных воздействий и обуславливает необходимость анализа состояния [3].

Основные направления, связанные с обнаружением аномалий, в основном, направлены на анализ внутренних характеристик устройств, сетевого взаимодействия, целостности программного обеспечения и информационной доступности. Однако наличие механических элементов КФС позволяет осуществлять развитие и

применение методов обнаружения физических воздействий на удаленные устройства, использующих анализ состояния мехатронных элементов [4–7].

Постановка задачи

Функционирование устройств предполагает наличие заранее запрограммированной реакции на различные внешние события, которая предусматривает предопределенную последовательность действий [8–10]. Каждая операция характеризуется внешними и внутренними процессами: потреблением мощности, электромагнитным излучением, звуком и т.д. [11–14]. Последовательность значений характеристик внешних и внутренних процессов таких действий образует поведенческий паттерн для выполнения заранее определенных команд [15]. Совокупность значений характеристик по времени дает различные оцифрованные последовательности трасс сигналов, на основе которых можно определить состояние объекта.

В целях идентификации состояния мехатронных устройств «Индустрии 4.0» рассматриваются оцифрованные дискретные значения трасс выборочных процессов:

$$y = \begin{Bmatrix} y_0^1 & \dots & y_{k-1}^1 \\ & \dots & \\ y_0^r & \dots & y_{k-1}^r \end{Bmatrix} \quad (1)$$

Использование процессов синхронизации по времени позволяет определить длины всех трасс равными K.

Таким образом, имеется поведенческий паттерна оцифрованных трасс Y вида $y = [y_0^{(1)} \dots y_k^r]$ и множество классов $C = \{C_0, \dots, C_n\}$. Существует целевая зависимость $c' : Y \to C$, значения которой известны на обучающей выборке $Y^R = (y^i, c^i)^{T_{i=1}}$. Требуется построить алгоритм классификации $a : Y \to C$, аппроксимирующую зависимость c' на всем множестве Y.

$$A(y) = \arg\max_j |\{r \in \{1,2,\dots,k\} f(y^r) = j\}| \quad (2)$$

Предлагаемый подход

В целях определения состояния мехатронных элементов и узлов используются разнообразные показатели оценки объекта. В качестве информационных каналов может рассматриваться амплитуда, частота, энергия другие параметры трасс сигналов, которые поступают в базу данных. Информация о состоянии объекта и сопоставление соответствующих значений дает возможность сформировать обучающую выборку, на основе которой возможно обнаружения аномалий.

Предлагаемый подход состоит из следующих шагов.

Шаг 1: подготовка базы данных и предварительный выбор оцифрованных значений сигнальных трасс.

Этот этап включает перевод устройства в заданный режим функционирования, сбор, объединение, интеграцию, структурирование и организацию базы данных поведенческих паттернов для обеспечения ее готовности к последующему анализу.

Шаг 2: предварительная обработка данных.

На данном этапе осуществляется анализ полученных на предыдущем шаге оцифрованных последовательностей с целью устранения различных шумов, выявленных при сборе данных.

Шаг 3: кластеризация.

Выбор метода кластеризации. Создание кластеров на основе данных о состояниях, полученных в результате обработки трасс оцифрованных последовательностей. Выбор методов идентификации состояния устройства и его элементов.

Шаг 4: идентификация состояний на основе данных кластера.

Обработка поступающих текущих данных оцифрованных последовательностей от устройства и анализ на основе метрик и процедур выбранного метода кластеризации текущего состояния.

На рис. 1 представлена иллюстрация последовательности действий идентификации состояния.

Эксперимент

Проведение эксперимента основывалось на паттерне, состоящем из синхронизированных последовательностей координат, получаемых от акселерометра данных. В результате, состояние анализируемого устройства идентифицировалось процессами распознавания оцифрованных значений трасс сигналов в 1000 значений по каждой координатной оси. Времена записей трасс синхронизированы и содержат значения амплитуд при изменении состояний сигналов.

Данные параметров ускорения и движения определялись акселерометром, находящимся на подвижной части манипулятора.

Схема проведения эксперимента представлена на рис. 2.

Обучающая и тестовые выборки содержали оцифрованные последовательности сигналов акселерометра для состояний: S_1 – движения манипулятора вперед и назад, S_2 – движения вперед влево, S_3 – движения вперед вправо. Для выявления отклонений были реализованы два «аномальных» состояния: S_4 – движения вперед влево с помехой, S_5 – движения вперед вправо с помехой. Продолжительность состояний также различалась по времени и составляла от 3,5 до 4,0 секунд.

Классифицируемые данные представлены в виде кортежей значений, полученных по разным информационным каналам, синхронизированных по времени.

$$Y(t) = \{(y_0(t_0), y_1(t_0), \dots, y_k(t_0)); (y_0(t_1), y_1(t_1), \dots, y_k(t_1)); \dots; (y_0(t_r), y_1(t_r), \dots, y_k(t_r))\} \quad (3)$$

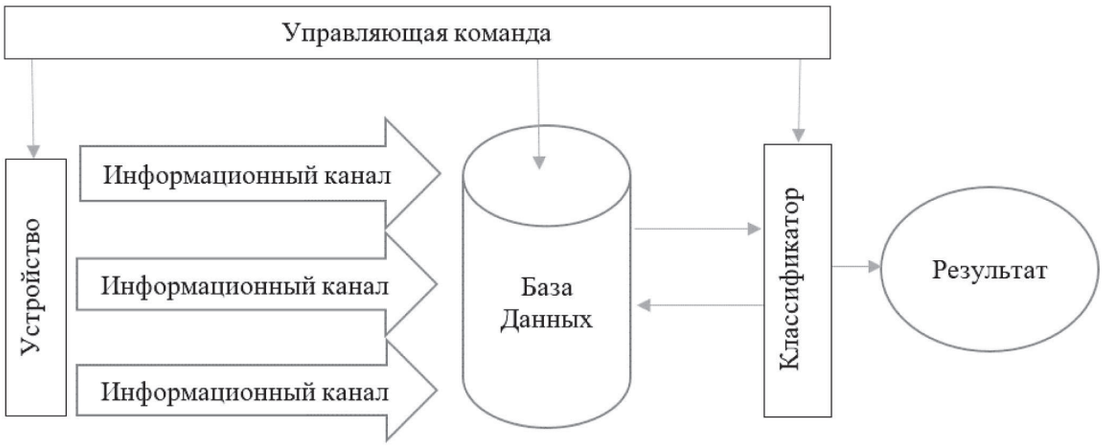


Рис. 1. Последовательность действий при идентификации состояния

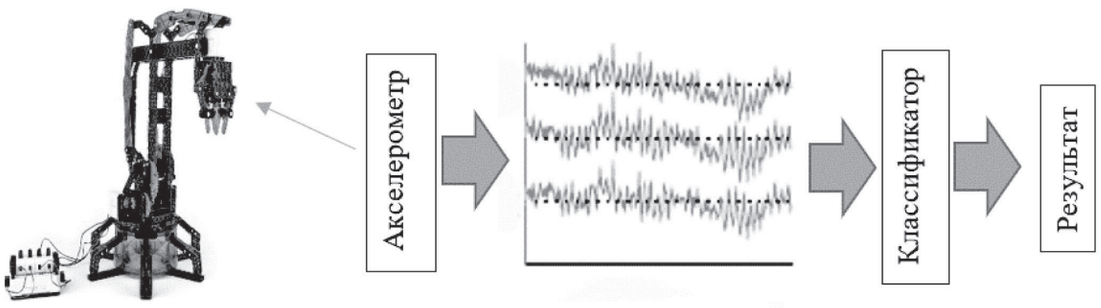


Рис. 2. Схема проведения эксперимента

где $Y(t)$ – кортеж значений $y_i(t_i)$ оцифрованных последовательностей от различных информационных каналов по времени.

Оцифрованные последовательности от различных источников формируют условный поведенческий паттерн состояния устройств. Содержащаяся в нем информация характеризует состояние устройства при получении типовой команды и позволяет производить анализ аномальных отклонений.

Обучающая выборка формировалась для различных состояний $S_1 - S_5$. На рис. 3 представлена информация, полученная при оцифровке данных проекций ускорения от акселерометра для различных состояний.

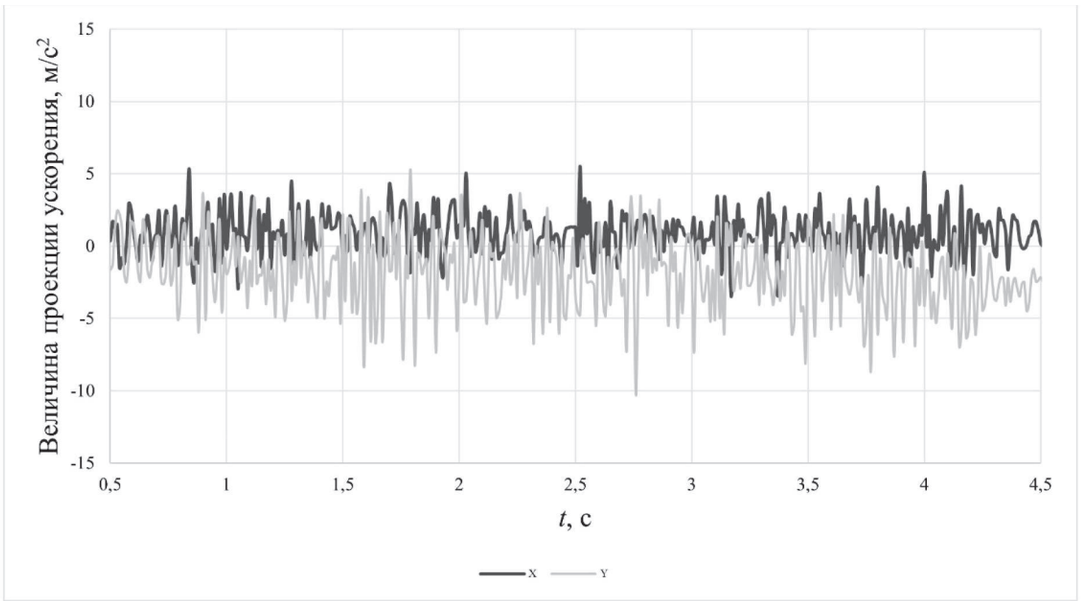
Анализ данных, полученных от оцифрованных последовательностей трасс, показывает их однородность и ярко выраженную скученность групп. Количество кластеров соответствует количеству определяемых состояний. Метод кластеризации *k-means* позволил разделить n наблюдений оцифрованных последовательностей трасс сигналов на k неперекрывающихся кластеров по состояниям.

В качестве меры близости для числовых атрибутов использовано Евклидово расстояние:

$$\rho(x, y) = \| x - y \| = \sqrt{\sum_{\rho=1}^{n} (x_\rho - y_\rho)^2}$$

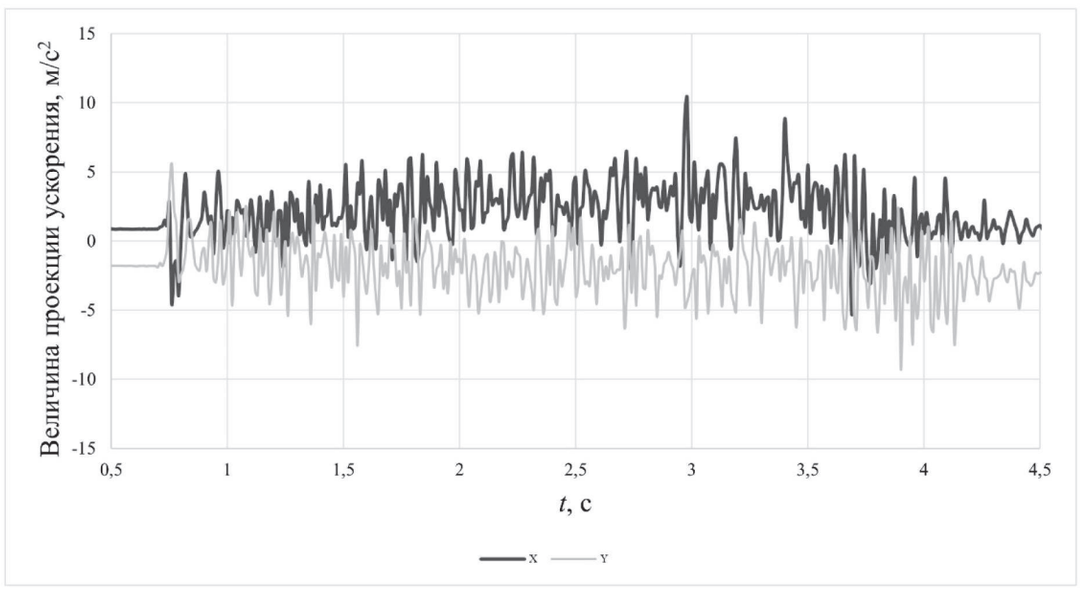
где $x, y \in R^n, R$ – пространство наблюдений.

С помощью значений обучающей выборки на основе метода k-средних произведено разделение m наблюдений на k групп (или кластеров) $(k \le m), S = \{S_1, S_2, ..., S_k\}$ так, чтобы минимизировать суммарное квадратичное отклонение точек кластеров от центроидов этих кластеров:

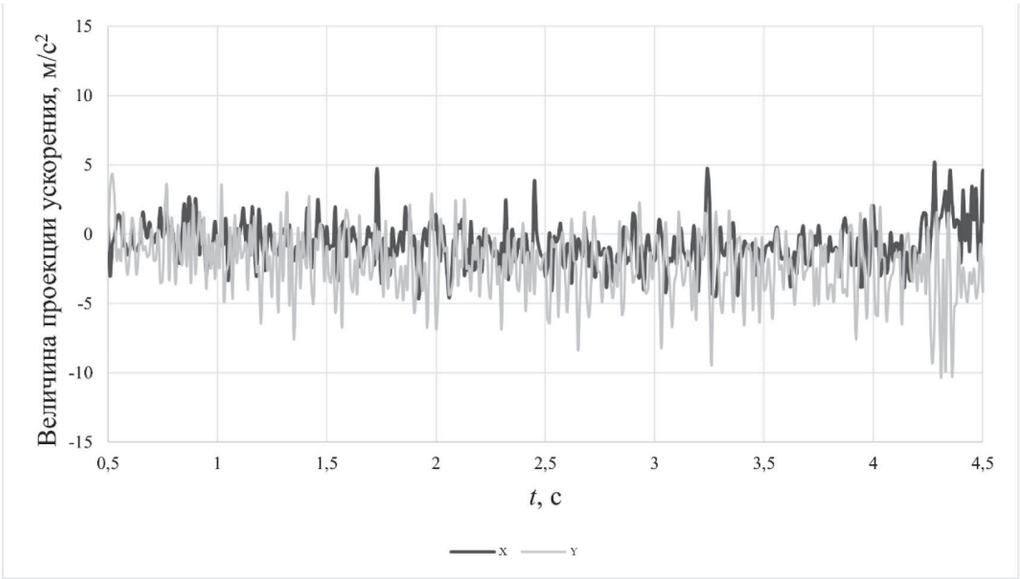


0ор

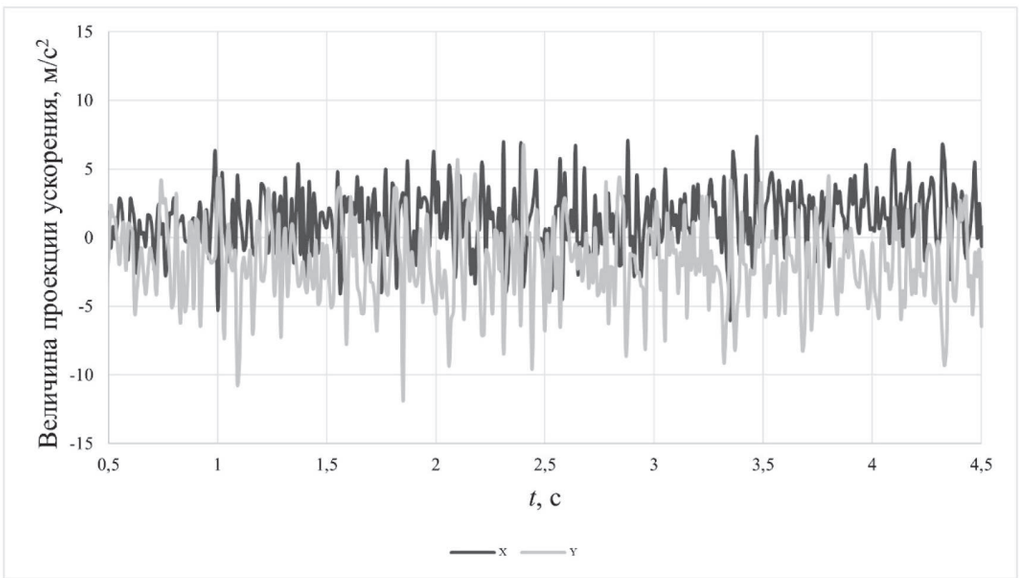
(*а*)



(*б*)



(*б*)



(*г*)

Рис. 3. График проекций ускорения для состояний: S_1 (*а*), S_2 (*б*), S_3 (*в*), S_4 (*г*)

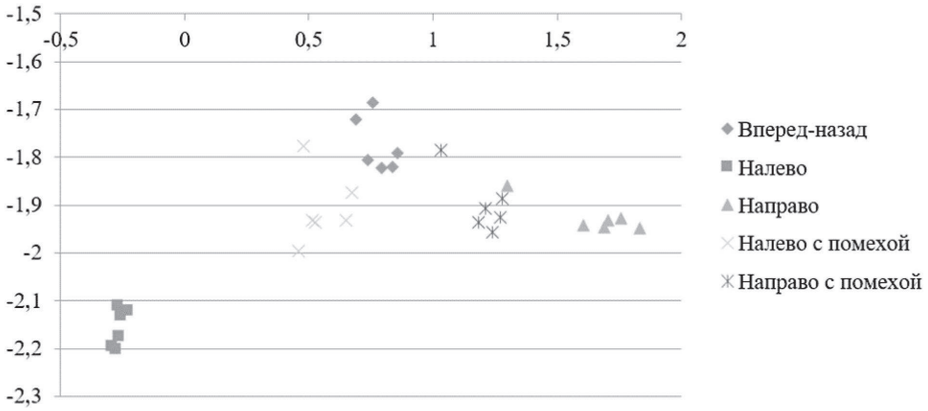


Рис. 4. Результаты кластеризации на основе среднего значения изменения координат

Таблица 1

Результаты анализа состояния на основе поиска ближайшего центроида кластеров *k-means*

		Прогнозируемое состояние				
		S_1	S_2	S_3	S_4	S_5
Реальное состояние	S_1	421	10	5	1	12
	S_2	5	471	17	0	3
	S_3	1	11	473	13	1
	S_4	7	12	55	419	6
	S_5	20	29	7	2	430

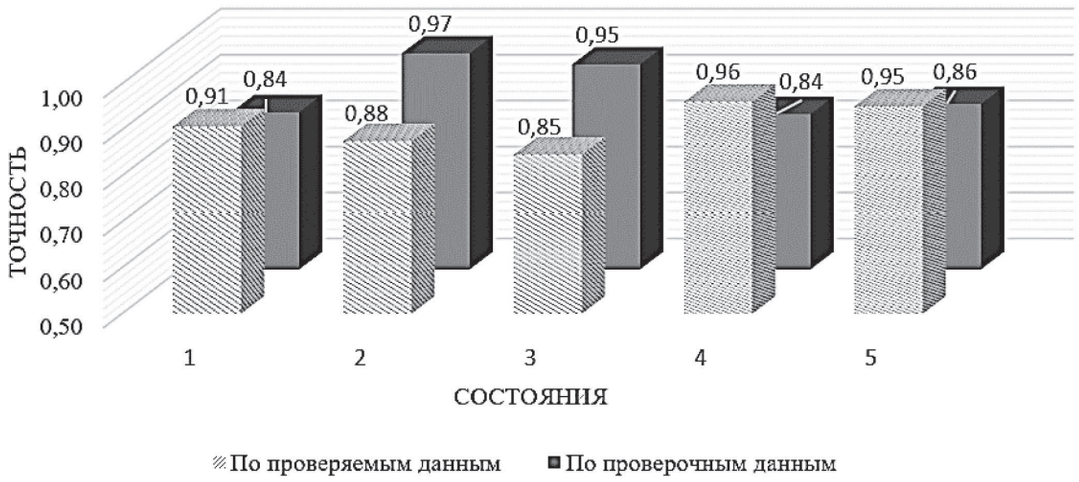


Рис. 5. Результаты классификации

$$\min[\sum_{i=1}^{k}\sum_{x}(S)_{\in S_i}\left\|x^{(j)}-\mu_i\right\|^2] \quad (5)$$

где $x^{(j)} \in R^n, \mu_i \in R^n, \mu_i$ – центроид для кластера S_i.

На рис. 4 представлены кластеры состояний, прослеживаются сгустки, которые достаточно хорошо отличимы друг от друга, размер кластеров обладает схожестью

Появление новых оцифрованных последовательностей проходит обработку, затем расстояние сравнивается с центроидами кластеров. В результате выбирается кластер, расстояние до центра которого минимально.

Результаты анализа состояния приведены в таблице 1.

Сумма значений диагональных элементов показывает общее количество правильно отнесенных к соответствующему кластеру состояний. Общая точность выбранного метода для случая полной классификации составила 0,90.

На рис. 5 приведены результаты классификации в виде точности отнесения по классам по проверяемым и проверочным данным.

Выводы

В данной работе представлен подход к идентификации состояния мехатронного устройства киберфизической системы «Индустрии 4.0» путем кластеризации информации в базах данных оцифрованных последовательностей трасс сигналов. С его помощью есть возможность определять аномальные состояния устройств, связанные с их функционированием.

Основным достоинством предложенного подхода является его простота и высокое быстродействие. Таким образом, распознавание по пяти состояниям демонстрирует возможность применения предложенного подхода, при этом происходит обнаружение с приемлемыми значениями точности идентификации.

Литература

1. Chopra, A. Paradigm shift and challenges in IoT security. / A. Chopra // Journal of Physics: Conference Series. – 2020. – Vol. 1432. – P. 012083.

2. Оценка рисков киберфизических систем с использованием моделирования доменов и имитационного моделирования / А.А. Тейланс [и др.] // Труды СПИИРАН. – 2018. – № 4 (59). – С. 115–139.

3. Горбачев, И. Е. Моделирование процессов нарушения информационной безопасности критической инфраструктуры / И.Е. Горбачев, А.П. Глухов // Труды СПИИРАН. – 2015. – № 1 (38). – С. 112–135.

4. Семенов, В. В. Обработка сигнальной информации в задачах мониторинга информационной безопасности автономных объектов беспилотных систем / В.В. Семенов, И.С. Лебедев // Научно-технический вестник информационных технологий, механики и оптики. – 2019. – Т. 19, № 3. – С. 492–498.

5. Сухопаров, М. Е. Мониторинг информационной безопасности элементов киберфизических систем с использованием искусственных нейронных сетей / М.Е. Сухопаров, В.В. Семенов, И.С. Лебедев // Методы и технические средства обеспечения безопасности информации. – 2018. – № 27. – С. 59–60.

6. Салахутдинова, К. И. Исследование влияния выбора признака и коэффициента (ratio) при формировании сигнатуры в задаче по идентификации программ / К.И. Салахутдинова [и др.] // Проблемы информационной безопасности. Компьютерные системы. – 2018. – № 1. – С. 136–141.

7. Using preventive measures for the purpose of assuring information security of wireless communication channels / I. Lebedev [et al.] // Proceedings of the 18th Conference of Open Innovations Association FRUCT and Seminar on Information Security and Protection of Information Technolog, FRUCT-ISPIT 2016, 2016. – P. 167–173.

8. Fruition of CPS and IoT in Context of Industry 4.0 / M. Devesh [et al.] // Advances in Intelligent Systems and Computing. – 2020. – Vol. 989. – P. 367–375.

9. Page, J. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities / J. Page, A. Zaslavsky, M. Indrawan // Proceedings of the First International Workshop on Safety and Security in Multiagent Systems (SaSeMAS 2004), 2004. – P. 85–101.

10. Семенов, В. В. Идентификация состояния отдельных элементов киберфизических систем на основе внешних поведенческих характеристик / В.В. Семенов, И.С. Лебедев, М.Е. Сухопаров // Прикладная информатика. – 2018. – Т. 13, № 5 (77). – С. 72–83.

11. Introduction to the Special Section on Electromagnetic Information Security / Y.I. Hayashi [et al.] // IEEE Transactions on Electromagnetic Compatibility. – 2013. – Vol. 55, No. 3. – P. 539–546.

12. Kocher, P. Introduction to differential power analysis and related attacks / P. Kocher, J. Jaffe, B. Jun // Proceedings of the CRYPTO'98, 1998, 1998. – P. 104–113.

13. Gerson de Souza, F. Differential audio analysis: a new side-channel attack on PIN pads / F. Gerson de Souza, H.Y. Kim // International Journal of Information Security. – 2019. – No. 18 (1). – P. 73–84.

14. A side-channel attack on smartphones: Deciphering key taps using built-in microphones / H. Gupta [et al.] // Journal of Computer Security. – 2018. – Vol. 26 (2). – P. 255–281.

15. Spatz, D. A review of anomaly detection techniques leveraging side-channel emissions / D. Spatz, D. Smarra, I. Ternovskiy // Proceedings of SPIE – The International Society for Optical Engineering, 2019. – Vol. 11011.