УДК 004.021 DOI: 10.17587/it.27.72-77

М. Е. Сухопаров, канд. техн. наук, ст. науч. сотр., e-mail: mikhailsukhoparov@yandex.ru,
НПК "ТРИСТАН",
И. С. Лебедев, д-р техн. наук, гл. науч. сотр., e-mail: lebedev@iias.spb.su,
К. И. Салахутдинова, мл. науч. сотр., e-mail: kainagr@mail.ru,
Санкт-Петербургский институт информатики и автоматизации РАН

Метод идентификации состояния информационной безопасности устройств интернета вещей

Описан подход к анализу состояния информационной безопасности устройств промышленного интернета и интернета вещей за счет применения внешних контролирующих систем, использующих побочные каналы и позволяющих уйти от потребления вычислительных ресурсов функционирующих устройств. Предлагаемое решение позволяет в оперативном режиме отслеживать состояние устройства с минимальными затратами на использование вычислительных ресурсов в ходе эксплуатации.

Ключевые слова: *интернет вещей, киберфизические системы, идентификация состояния, информационная безопасность, побочные каналы*

Введение

Современная парадигма интернета вещей (Internet of Things, IoT) определяет концепцию развития общедоступных сетей информационных, телекоммуникационных и киберфизических систем. Происходит стремительный рост числа устройств, датчиков, сенсоров, подключаемых к сетевой инфраструктуре. Используемые подходы и методы интернета вещей связаны с интеллектуализацией процессов функционирования, передачи информации, сбора и обработки разнородных данных. Это достигается благодаря развитию технологий идентификации и мягкой настройки устройств и узлов, передачи, обработки данных, которые обеспечивают увеличение скорости, устранение избыточности передаваемых сообщений. Используемые в IoT оконечные устройства и датчики, в основном, не обладают большими вычислительными мощностями, поэтому эффект быстродействия обеспечивается упрощением ряда технологических процессов, в том числе обеспечивающих информационную безопасность узлов и элементов интернета вещей.

В связи с этим возникает определенное противоречие, поскольку, с одной стороны, возникает потребность в реализации высокоэффективного встраиваемого программного обеспечения, реализующего методы искусственного интеллекта, машинного обучения, обработки разнородных данных, а с другой, имеются условия ограничений вычислительных ресурсов и необходимость реализации процессов обеспечения информационной безопасности критически важных узлов инфраструктуры.

Существующие подходы

Унифицированные решения интернета вещей можно найти как в обычных бытовых приборах, так и в промышленных системах управления и мониторинга сетей промышленных объектов, производств, государственных учреждений [1].

Доступность, относительно небольшая стоимость, широкое применение встраиваемых элементов устройств делает возможным использование различных методов реверс-инжиниринга в целях модификации программной и аппаратной частей, встраивания "функционала", необходимого для реализации различных деструктивных воздействий, что может приводить к утечкам конфиденциальной информации, к катастрофическим системным сбоям [2—5]. Имеется достаточное число примеров, когда для осуществления распределенных атак

типа "отказ в обслуживании" (DDoS), организации ботнетов использовались обычные роутеры, веб-камеры и принтеры [5—7]. Произошедшие инциденты определили значительный интерес к разработке и реализации решений по обеспечению безопасности встроенных устройств интернета вещей, среди которых можно выделить несколько направлений.

Один из основных подходов связан с мониторингом состояния информационной безопасности устройств, узлов и сегментов информационно-телекоммуникационных сетей на основе статистических параметров функционирования. Обнаружение атаки во время выполнения рассматривается как задача обнаружения аномального состояния, для чего применяется хорошо зарекомендовавший себя научно-методический аппарат марковских моделей, нейронных сетей, опорных векторов [8, 10].

Однако анализ состояния на основе статистической информации доступной в процессе функционирования, ориентирован на внешние признаки и не позволяет обнаружить аномальные ситуации, возникающие на программном уровне, например, переполнение буфера [7]. Для этого используются решения, связанные с реализацией мониторов, отслеживающих информацию о выполнении сегментов кода [7, 10]. Применение таких средств может негативно влиять на производительность устройств, распределение вычислительных ресурсов и стоимость. При осуществлении атаки злоумышленник пытается в первую очередь отключить систему защиты.

Вместе с тем, существуют побочные каналы, которые могут использоваться как для атаки на устройство, так и для построения систем мониторинга информационной безопасности [9]. Подобные подходы используют временные ряды, полученные от регистрирующих устройств, фиксирующих в процессе функционирования электромагнитное излучение, изменения потребляемой мощности, напряжения, загрузки вычислительных ресурсов и т.д. для мониторинга аномальных состояний [11].

Таким образом, дальнейшее развитие методов анализа состояния информационной безопасности предполагает использование большого спектра различных информационных каналов.

Предлагаемый подход

В целях идентификации состояния информационной безопасности возникает необходимость анализа ряда процессов по временным рядам, регистрируемым различными датчиками. Современные устройства промышленного интернета и интернета вещей имеют ограниченный функционал и вычислительные ресурсы, производительность которых обеспечивает выполнение возложенных на них функциональных задач. Внедрение мониторов состояния и дополнительных защитных функций не всегда возможно. Поэтому одним из направлений решения поставленных проблемных вопросов является применение внешних контролирующих систем, использующих сторонние (побочные) каналы, не потребляющих вычислительные ресурсы функционирующих устройств.

В процессе функционирования сети происходит множество процессов, связанных с приемом, передачей, обработкой сообщений, реализацией вычислительных и других алгоритмов. Это вызывает одновременную смену множества параметров. Путем регистрации их значений и синхронизации по времени полученных значений от различных мониторов, датчиков и сенсоров можно определить временные ряды, связанные с процессом, поступающие от регистрирующих устройств.

Идентификация состояния IoT-устройства происходит на основе значений, определяемых в дискретные моменты времени t_0, t_1, ..., t_n. В целях повышения качества анализируемых данных предполагается, что временной ряд должен имеет постоянную длину [12]. В результате по каждому состоянию получаем описания, выраженные m-мерными векторами признаков $X = (X_1, X_2, ..., X_m)$.

Множество рассматриваемых состояний C определяется заранее, что позволяет разметить обучающую выборку векторов X и определить два множества опасного и безопасного состояний $\{C_1, C_2\} \in C$

По очередным поступающим значениям вектора признаков $X = (X_1, X_2, ..., X_m)$ проводится идентификация класса C_i, $i = 1, 2$. Строится решающее правило для алгоритма $\rho(x)$, которое ставит в соответствие наблюдению одно из множеств C_1 или C_2. Оно определяется функцией $\varphi(x)$, порождающей разбиение пространства на две непересекающиеся области:

$$\rho(x) = \begin{cases} C_1, \text{ при } \varphi(x) \geqslant \varepsilon; \\ C_2, \text{ при } \varphi(x) < \varepsilon, \end{cases} \quad (1)$$

где ε — пороговое значение.

Экспериментальная оценка

При проведении экспериментальной оценки рассматривали работу двух программ, потребляющих вычислительные ресурсы.

Целью проведения эксперимента было выявление состояния вычислительного узла, определяемого алгоритмом обработки данных, на основе оцифрованных показателей загрузки вычислительных ресурсов [13—16]. В качестве временных рядов, описывающих состояния, использовались синхронизированные по времени процентные показатели монитора системной загрузки.

В качестве основного метода оценки рассматривается один из наиболее популярных алгоритмов кластеризации k-means. Он включает ряд шагов:

1) первоначально определяется число рассматриваемых состояний. Определяется размер анализируемых временных рядов, поступающих от монитора загрузки. Подготавливается обучающая выборка, где заданные состояния заранее размечаются;

2) анализируемые состояния разделяются на два подмножества: безопасные, где выполняются заранее предопределенные процессы, и опасные — где имеются отклонения от параметров в заданных режимах работы;

3) на основе обучающей выборки по мере поступления различных временных рядов определяются начальные центры их кластера:

$$\arg\min_S \sum_{i=1}^{k} \sum_{x \in S_i} \rho(x, \mu_i)^2, \qquad (2)$$

где μ_i — центры кластеров, $i = 1, ..., k$; $\rho(x, \mu_i)$ — функция расстояния между x и μ_i;

4) по мере поступления дополнительных значений временных рядов определяется ближайший центр кластера, вычисляются центроида и смещение центра кластера;

5) дальнейший анализ происходит на основе сравнений полученных текущих значений устройства с эталонными значениями центров кластеров и классов, вычисленными в условиях формировании обучающей выборки.

Рассмотрим четыре состояния:

S_0 — состояние, где работают фоновые процессы — устройство не выполняет полезные вычислительные действия;

S_1 — функционирует только алгоритм 1;

S_2 — функционирует только алгоритм 2;

S_3 — запущены обе программы, реализующие алгоритм 1 и алгоритм 2.

Каждое состояние определяется временным рядом, показывающим загрузку центрального процессора и памяти. Вид временного ряда для различных состояний представлен на рис. 1, *а—г*.

При проведении эксперимента была получена выборка временных рядов для рассматриваемых состояний. Выборка была разделена на обучающую и тестовую. Идентификацию состояния выполняли на основе метода кластеризации k-means [17, 18]. На обучающей выборке были размечены состояния, что позволило определить центры кластеров μ_i $i = 1, 2, ..., 4$, а поступающие значения тестовой выборки оценивали исходя из метрики расстояния и соотносили с соответствующим кластером.

В качестве меры близости использовано евклидово расстояние:

$$\rho(x, \mu_i) = \sqrt{\sum_{r=1}^{n} (x_r - \mu_i)^2}, \qquad (3)$$

где R — пространство наблюдений; $x, \mu_i \in R^n$.

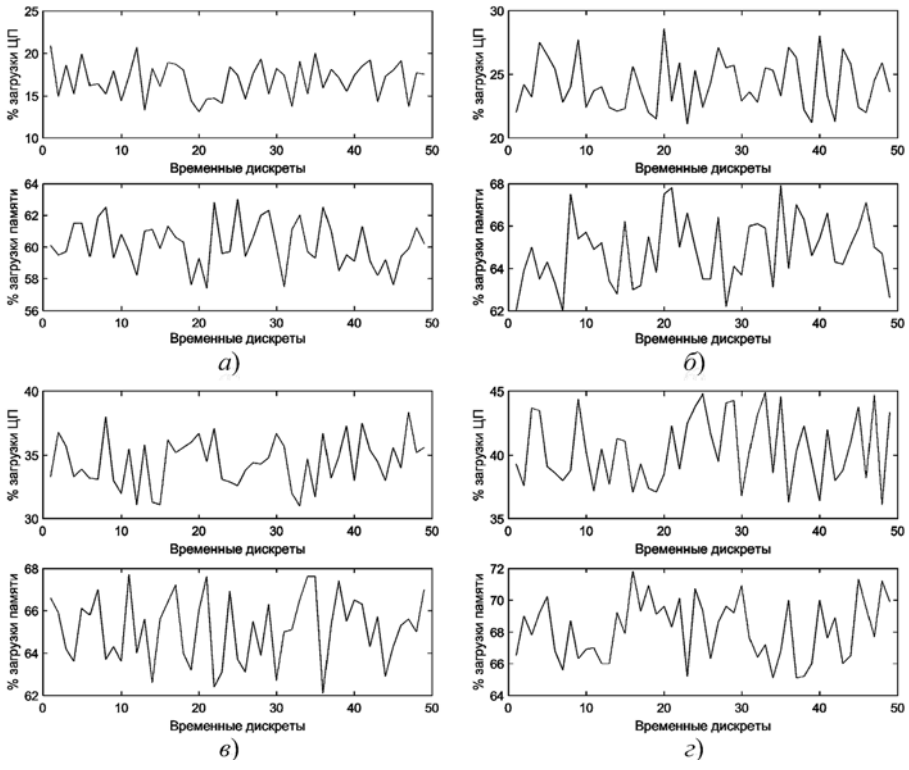

Рис. 1. Загрузка процессора и памяти для состояния:
а — S_0; *б* — S_1; *в* — S_2; *г* — S_3

Рассматривая двумерные значения загрузки процессора и памяти как обучающую выборку, для состояний S_0, ..., S_4 получаем кластеры, представленные на рис. 2.

Измерив расстояние до центроидов, выбираем из них минимальное значение, на основе которого принимаем решение о принадлежности к кластеру, идентифицирующему состояние:

$$Sh(x^{(j)}) = \frac{b(x^{(j)}) - a(x^{(j)})}{\max(a(x^{(j)}), b(x^{(j)}))}, \qquad (4)$$

где $a(x^{(j)})$ — среднее значение от точки $x^{(j)}$ до других точек кластера; $b(x^{(j)})$ — минимум (по другим кластерам) средних значений расстояний от точки $x^{(j)}$ до точек другого кластера.

Визуализация оценки полученных кластеров приведена на рис. 3.

Временные ряды от центрального процессора и ресурсов памяти для различных состояний позволяют формировать достаточно хорошо отличимые друг от друга кластеры.

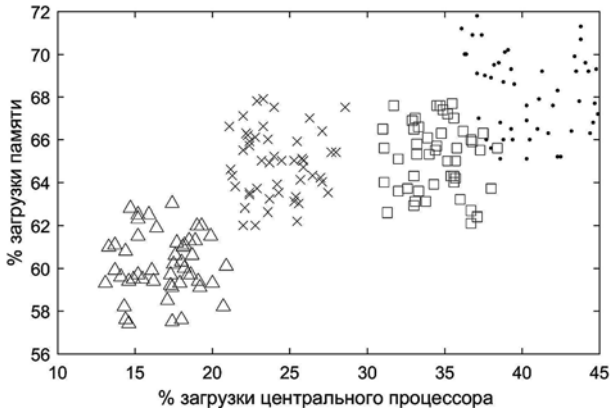

Рис. 2. Результаты кластеризации на основе метода кластеризации k-means

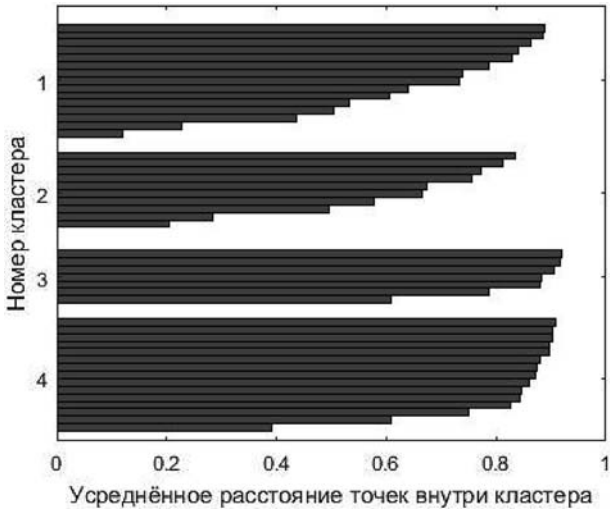

Рис. 3. Визуализация оценки полученных кластеров

Заключение

В настоящее время в связи с развитием интернета вещей возникает проблема оценки состояния информационной безопасности огромного числа устройств, находящихся вне контролируемой зоны. В качестве одного из методов был выбран и рассмотрен метод идентификации состояния на основе метода кластеризации k-means, обрабатывающего временные ряды от регистрирующих устройств. Новизна состоит в том, что представленный метод идентификации состояния информационной безопасности устройства, базирующийся на анализе временных рядов, позволяет в оперативном режиме отслеживать состояние устройства с минимальными затратами на использование вычислительных ресурсов в ходе эксплуатации.

Характерными особенностями представленного решения являются его простота реализации и модификации.

Применение метода существенно зависит от обрабатываемых данных. Скорость и точность обработки связаны с выбором центройдов кластеров, размером поступающего на вход временного ряда, отсутствием "выбросов" данных. Основной вопрос состоит в том, чтобы найти такие центры, для которых сформированные кластеры были бы компактны, что позволит достигать заданных показателей точности.

Список литературы

1. **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. 2017 ACM SIGSAC Conf. Computer and Communications Security. P. 1095—1108.

2. **Garcia L., Brasser F., Cintuglu M. H., Sadeghi A.-R., Mohammed O., Zonouz S. A.** Hey, my malware knows physics! Attacking PLCs with physical model aware rootkit // Proc. Network and Distributed System Security Symp. San Diego, CA. 2017. P. 26—28.

3. **Slay J., Miller M.** Lessons learned from the Maroochy water breach // Proc. Int. Conf. Critical Infrastructure Protection. 2007. P. 73—82.

4. **Falliere N., Murchu L. O., Chien E.** "W32. Stuxnet dossier // Symantect Security Response. 2011. Vol. 5, N. 6. P. 29.

5. **Bertino E., Islam N.** Botnets and Internet of Things security // Computer. 2017. Vol. 50, N. 2. P. 76—79.

6. **McLaughlin S. E., Zonouz S. A., Pohly D. J., McDaniel P. D.** A trusted safety verifier for process controller code // Presented at the Network and Distributed System Security Symp., San Diego, CA. Feb. 23—26. 2014.

7. **Qiao Y., Xin X., Bin Y., Ge S.** Anomaly intrusion detection method based on HMM // Electron. Lett. 2002. Vol. 38, N. 13. P. 663—664.

8. **Ryan J., Lin M.-J., Miikkulainen R.** Intrusion detection with neural networks // Advances Neural Inform. Process. Syst. 1998. P. 943—949.

9. **Etigowni S., Tian D. J., Hernandez G., Zonouz S., Butler K.** CPAC: Securing critical infrastructure with cyber-physical

access control // Proc. 32nd Annu. Conf. Computer Security Applications. 2016. P. 139—152.

10. **Farwell J. P., Rohozinski R.** Stuxnet and the Future of Cyber War // Survival. 2011. Vol. 53:1. P. 23—40.

11. **Yeung D.-Y., Ding Y.** Host-based intrusion detection using dynamic and static behavioral models // Pattern recognition. 2003. Vol. 36, N. 1. P. 229—243.

12. **Igure V., Laughter S., Williams R.** Security issues in SCADA networks // Computers & Security. 2006. Vol. 25, 7. P. 498—506.

13. **Зикратов И. А., Зикратова Т. В., Лебедев И. С.** Доверительная модель информационной безопасности мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2 (90). С. 47—52.

14. **Gao D., Reiter M., Song D.** Beyond output voting: Detecting compromised replicas using HMM-based behavioral distance // IEEE Transactions on Dependable and Secure Computing. 2009. Vol. 6, N. 2. P. 96—110.

15. **Bevir M. K., O'Sullivan V. T., Wyatt D. G.** Computation of electromagnetic flowmeter characteristics from magnetic field data // Journal of Physics D Applied Physics. 1981. Vol. 14(3). P. 373—388.

16. **Semenov V. V., Lebedev I. S., 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.

17. **Семенов В. В., Лебедев И. С., Сухопаров М. Е.** Подход к классификации состояния информационной безопасности элементов киберфизических систем с использованием побочного электромагнитного излучения // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18, № 1. С. 98—105.

18. **Сухопаров М. Е., Семенов В. В., Салахутдинова К. И., Лебедев И. С.** Выявление аномального функционирования устройств индустрии 4.0 на основе поведенческих паттернов // Проблемы информационной безопасности. Компьютерные системы. 2020. № 1 (41). С. 96—102.

19. **Бендат Д., Пирсол А.** Применение корреляционного и спектрального анализа. М.: Мир, 1983. 312 с.

20. **Засов В. А., Тарабардин М. А., Никоноров Е. Н.** Алгоритмы и устройства для идентификации входных сигналов в задачах контроля и диагностики динамических объектов // Вестник Самарского государственного аэрокосмического университета. 2009. № 2. С. 115—123.

21. **Lockhart D. J.** et al. Expression monitoring by hybridization to high-density oligonucleotide arrays // Nat. Biotechnol. 1996. Vol. 14. P. 1675—1680.

22. **Golub T. R.** Molecular classification of cancer: class discovery and class prediction by gene expression monitoring // Science. 1999. Vol. 286 (5439). P. 531—537.

23. **Anderberg M. R.** Cluster Analysis for Applications. New York: Academic Press, 1976. 376 p.

24. **Dembele D., Kastner P.** C-means method for clustering microarray data // Bioinformatics. 2003. Vol. 19 (8). P. 973—980.

25. **Rousseeuw J. P.** Silhouettes: a graphical aid to the interpretation and validation of cluster analysis // J. Comp. Appl. Math. 1987. Vol. 20. P. 53—65.

26. **Whitfield M. L.** et al. Identification of Genes Periodically Expressed in the Human Cell Cycle and Their Expression in Tumors // Mol. Biol. Cell. 2002. Vol. 13. P. 1977—2000.

M. E. Sukhoparov, Ph.D. of Engineering Sciences, e-mail: mikhailsukhoparov@yandex.ru,
NPK "TRISTAN", St. Petersburg, 195256, Russian Federation,
I. S. Lebedev, Advanced Doctor in Engineering Sciences, e-mail: lebedev@iias.spb.su,
K. I. Salakhutdinova, Research Assistant, e-mail: kainagr@mail.ru,
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
St. Petersburg, 199178, Russian Federation

Method for Identifying the Information Security Status of Internet of Things Devices

An approach to analyzing the state of information security of industrial Internet devices and the Internet of things is described. External control systems that use side channels and allow to avoiding the consumption of computing resources of functioning devices are used. The proposed solution allows one to monitor the state of the device on-line with minimal costs for using computing resources during operation.

Keywords: *Internet of things, cyber-physical systems, state identification, information security, side channels*

DOI: 10.17587/it.27.72-77

References

1. **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. 2017 ACM SIGSAC Conf. Computer and Communications Security*, pp. 1095—1108.

2. **Garcia L., Brasser F., Cintuglu M. H., Sadeghi A.-R., Mohammed O., Zonouz S. A.** Hey, my malware knows physics! Attacking PLCs with physical model aware rootkit, *Proc. Network and Distributed System Security Symp.*, San Diego, CA, 2017, pp. 26—28.

3. **Slay J., Miller M.** Lessons learned from the Maroochy water breach, *Proc. Int. Conf. Critical Infrastructure Protection*, 2007, pp. 73—82.

4. **Falliere N., Murchu L. O., Chien E.** W32. Stuxnet dossier, *Symantecm Security Response*, 2011, vol. 5, no. 6, p. 29.

5. **Bertino E., Islam N.** Botnets and Internet of Things security, *Computer*, 2017, vol. 50, no. 2, pp. 76—79.

6. **McLaughlin S. E., Zonouz S. A., Pohly D. J., McDaniel P. D.** A trusted safety verifier for process controller code, *presented at the Network and Distributed System Security Symp.*, San Diego, CA, 2014, Feb. 23—26.

7. **Qiao Y., Xin X., Bin Y., Ge S.** Anomaly intrusion detection method based on HMM, *Electron. Lett.*, 2002, vol. 38, no. 13, P. 663—664.

8. **Ryan J., Lin M.-J., Miikkulainen R.** Intrusion detection with neural networks, *Advances Neural Inform. Process. Syst.*, 1998, pp. 943—949.

9. **Etigowni S., Tian D. J., Hernandez G., Zonouz S., Butler K.** CPAC: Securing critical infrastructure with cyber-physical access control, *Proc. 32nd Annu. Conf. Computer Security Applications*, 2016, pp. 139—152.

10. **Farwell J. P., Rohozinski R.** Stuxnet and the Future of Cyber War, *Survival*, 2011, vol. 53:1, pp. 23—40.

11. **Yeung D.-Y., Ding Y.** Host-based intrusion detection using dynamic and static behavioral models, *Pattern recognition*, 2003, vol. 36, no. 1, pp. 229—243.

12. **Igure V., Laughter S., Williams R.** Security issues in SCADA networks, *Computers & Security,* 2006, vol. 25, no. 7, pp. 498—506.

13. **Zikratov I. A., Zikratova T. V., Lebedev I. S.** Trust model for information security of multi-agent robotic systems with a decentralized management, *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, vol. 2 (90), pp. 47—52 (in Russian).

14. **Gao D., Reiter M., Song D.** Beyond output voting: Detecting compromised replicas using HMM-based behavioral distance, *IEEE Transactions on Dependable and Secure Computing*, 2009, vol. 6, no. 2, pp. 96—110.

15. **Bevir M. K., O'Sullivan V. T., Wyatt D. G.** Computation of electromagnetic flowmeter characteristics from magnetic field data, *Journal of Physics D Applied Physics*, 1981, vol. 14(3), pp. 373—388.

16. **Semenov V. V., Lebedev I. S., 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, pp. 104—112.

17. **Semenov V. V., Lebedev I. S., Sukhoparov M. E.** Approach to classification of the information security state of elements for cyberphysical systems by applying side electromagnetic radiation, *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*., 2018, vol. 18, no. 1, pp. 98—105 (in Russian)..

18. **Sukhoparov M. E., Semenov V. V., Salakhutdinova K. I., Lebedev I. S.** Identification of anomalous functioning of industry 4.0 devices based on behavioral patterns, *Information Security Problems. Computer Systems,* 2020, no. 1 (41), pp. 96—102 (in Russian).

19. **Julius S. Bendat, Allan G. Piersol.** Engineering Applications of Correlation and Spectral Analysis, Moscow, Mir, 1983, 312 p. (in Russian).

20. **Zasov V. A., Tarabardin M. A., Nikonorov Y. N.** Algorithms and devices for input signal identification in problems of dynamic object control and diagnostics, *Vestnik of samara university. Aerospace and mechanical engineering*, 2009, no. 2, pp. 115—123 (in Russian).

21. **Lockhart D. J.** et al. Expression monitoring by hybridization to high-density oligonucleotide arrays, *Nat. Biotechnol.*, 1996, vol. 14, pp. 1675—1680.

22. **Golub T. R.** Molecular classification of cancer: class discovery and class prediction by gene expression monitoring, *Science*, 1999, vol. 286 (5439), pp. 531—537.

23. **Anderberg M. R.** Cluster Analysis for Applications, *Academic Press*, New York, 1976, 376 p.

24. **Dembele D., Kastner P.** C-means method for clustering microarray data, *Bioinformatics*, 2003, vol. 19 (8), pp. 973—980.

25. **Rousseeuw J. P.** Silhouettes: a graphical aid to the interpretation and validation of cluster analysis, *J. Comp. Appl. Math.*, 1987, vol. 20, pp. 53—65.

26. **Whitfield M. L.** et al. Identification of Genes Periodically Expressed in the Human Cell Cycle and Their Expression in Tumors, *Mol. Biol. Cell.*, 2002, vol. 13, pp. 1977—2000.