УДК 004.021

Идентификация состояния информационной безопасности устройств интернета вещей в информационно-телекоммуникационных системах

Сухопаров М. Е., Лебедев И. С.

Постановка задачи: *мониторинг состояния информационной безопасности устройств информационно-телекоммуникационных систем и сетей в концепции интернета вещей обусловливает необходимость поиска и совершенствования подходов к обнаружению различного вида угроз. Процессы унификации, типизации программно-аппаратной части устройств интернета вещей облегчают осуществление реверс-инжиниринга, направленного на модификацию программного и аппаратного обеспечения с целью блокировки отдельных встроенных защитных функций со стороны потенциального злоумышленника. Возникает необходимость разработки универсальных моделей и методов идентификации состояния информационной безопасности маломощных с вычислительной точки зрения устройств, использующих комплексные подходы анализа данных, поступающих от внутренних и внешних (сторонних) информационных каналов.* ***Целью работы*** *является разработка подхода к идентификации состояния информационной безопасности устройств интернета вещей на основе обрабатываемых временных рядов, регистрируемых от датчиков и сенсоров при выполнении различных процессов, внутренних и внешних (сторонних) источников.* ***Используемые методы:*** *решение задачи основано на методах кластеризации, методах классификации, а также применены элементы методов статистического анализа.* ***Новизна:*** *элементом новизны представленного решения является использование шаблонных последовательностей, зарегистрированных в сложившихся в прошлом условиях функционирования устройства интернета вещей, содержащих синхронизированные временные ряды, показывающие полученные от различных датчиков и сенсоров числовые значения во время выполнения процессов.* ***Результат:*** *подход к идентификации состояния информационной безопасности устройства интернета вещей в условиях ограничений вычислительных ресурсов.* ***Практическая значимость:*** *предлагаемый подход дает возможность идентифицировать состояние информационной безопасности устройства интернета вещей, не увеличивая объем хранящейся и обрабатываемой во внутренних ресурсах информации.*

Ключевые слова: *мониторинг состояния информационной безопасности, узлы и устройства интернета вещей, сетевая инфраструктура.*

Введение

Современный интернет вещей представляет концепцию организации и построения вычислительной сети физических предметов, взаимодействующих друг с другом и внешней средой. Использование технологий идентификации, измерения, передачи и обработки данных обуславливает необходимость создания различных систем защиты информации (СЗИ) и мониторинга состояния информационной безопасности (ИБ), направленных на нейтрализацию угроз для интернета вещей IoT (Internet of Things).

Библиографическая ссылка на статью:
Сухопаров М. Е., Лебедев И. С. Идентификация состояния информационной безопасности устройств интернета вещей в информационно-телекоммуникационных системах // Системы управления, связи и безопасности. 2020. № 3. С. 252-268. DOI: 10.24411/2410-9916-2020-10310.

Reference for citation:
Sukhoparov M. E., Lebedev I. S. Identification the Information Security Status for the Internet of Things Devices in Information and Telecommunication Systems. *Systems of Control, Communication and Security*, 2020, no. 3, pp. 252-268 (in Russian). DOI: 10.24411/2410-9916-2020-10310.

Важен комплексный подход к организации защиты подобных систем. Реализация СЗИ и мониторинга состояния ИБ информационно-телекоммуникационных систем и сетей строятся на обеспечении безопасности связи, контроля взаимодействия в сети, защиты устройств [1-3]. Однако подобные системы предполагают динамическое развитие и возникновение ситуаций, требующих анализа, когда происходит одновременное подключение и старых и новых устройств, используются разные версии прошивок, аппаратных и программных решений, применяется множество протоколов сопряжения, технологий обработки, анализа и передачи данных.

Реализующие функционал устройства IoT, в отдельных случаях, находятся вне контролируемой зоны, требуют контроля, обновления программного обеспечения, оптимизации ряда процессов функционирования в течение жизненного цикла. Встроенные системы защиты в подобных устройствах не всегда эффективны, т. к. потенциальные злоумышленники, обычно, не имеют затруднений к доступу и могут осуществлять поиск уязвимостей на типовых устройствах [4].

В ходе реализации информационных систем и сетей возникает необходимость совершенствования систем защиты, контроля и мониторинга информационной безопасности устройств интернета вещей, где, в качестве одного из направлений, помимо внутренних встраиваемых систем могут использоваться, например, акустические, электромагнитные и другие, напрямую не связанные с протекающими процессами, побочные, сторонние каналы, содержащие информацию о процессе [5-8].

Основу подобных решений составляет то, что множество элементов IoT обладают небольшими программно-аппаратными возможностями, заранее предопределенными действиями и реакциями, и, в течение жизненного цикла, в основном, не меняют свой ограниченный функционал. Многие устройства, сегменты IoT, имеют предельные допустимые значения параметров функционирования, выполняют запрограммированную последовательность на управляющие команды и внешние события, происходящие в информационной системе. На основе таких данных, применяя методы машинного обучения, статистического анализа, можно определить шаблоны функционирования, вычислить нормальное состояние, где функционируют заранее предопределенные процессы, и аномальное, связанное с появлением значений параметров и характеристик, показывающих отклонения от нормы. Таким образом, целью работы является разработка подхода к идентификации состояния информационной безопасности устройств интернета вещей на основе обрабатываемых временных рядов, регистрируемых от датчиков и сенсоров при выполнении различных процессов, внутренних и внешних (сторонних) источников.

Постановка задачи

Для формальной постановки и решения задачи в работе введены обозначения, представленные в таблице 1.

Очень часто системы и устройства представляют из себя «черный ящик». При разработке используются программные и аппаратные платформы разных

производителей, стандартные библиотеки, где не всегда можно анализировать исходный код или аппаратные прошивки. В большинстве случаев производители устройств IoT реализуют их как закрытые системы, где отсутствует возможность осуществлять изменения аппаратной или модификацию программной части.

Таблица 1 – Обозначения

Обозначение	Физический смысл обозначения
S	числовые последовательности (временные ряды)
t	момент времени
N	предельные значения и индексы, их, наверное, не надо указывать
m	предельные значения и индексы, их, наверное, не надо указывать
H	множество кортежей характеристик
Z	множество состояний устройства
C	множество классов состояний
r	расстояние между объектами
q	количество каналов источников
u	внешняя среда
h	переходная характеристика
v	шумовая составляющая
k	количество входов
d	количество выходов
i	регистрируемый канал
j	регистрирующий канал
X	вектор
ε	пороговое значение
R	пространство наблюдений
l	количество групп
μ	центроид
w	весовой коэффициент

Все механизмы защиты являются внутренними, в случае возникновения коллизий при проверке целостности включаются механизмы защиты вплоть до прекращения функционирования устройств. Однако в процессе эксплуатации возникает необходимость конфигурации, настройки, улучшения характеристик функционирования системы. Учитывая, что большинство элементов системы являются типовыми, где используются одинаковые алгоритмы функционирования, становится возможным проведение реверс-инжиниринга, поиск уязвимостей, попытки передачи широковещательных управляющих команд, осуществления различного рода деструктивных воздействий, переводящих в режимы работы, сопровождающиеся отклонением рабочих параметров от предельно-допустимых значений, что может существенно влиять на функции встроенных защитных механизмов. В связи с этим необходимо использовать одновременно несколько информационных каналов, которые могут быть как сторонними, так и внутренними.

Как и в любой системе, процессы устройств IoT протекают в динамике, одновременно меняется множество параметров, и в целях выявления аномалий приходится просматривать не одно, а несколько дискретных состояний, предшествующих анализируемой ситуации.

Предлагаемый подход связан с использованием поведенческих паттернов. Под паттерном понимается синхронизированное по времени множество последовательностей с определенной частотой снятия значений от внутренних и внешних датчиков, регистрирующих параметры протекающих в устройствах процессов. Поведенческий паттерн формируется на основе информации о функционировании устройства IoT и его компонент: загрузка и потребление ресурсов, данные о электромагнитных и звуковых спектрах, частоты и амплитуды вибраций, температура и т. д. [8, 9].

В определенные дискретные моменты времени в информационной системе регистрируются значения от измерительных устройств и сенсоров, фиксирующих протекающий процесс. Множество датчиков в моменты времени $t = 1, ..., N$ выдают числовые последовательности $\{S_0(t), S_1(t), ..., S_m(t)\}$. Синхронизируемые по времени и получаемые от различных контролирующих элементов значения в дискретные моменты времени определяют кортежи характеристик $H = \{S(t) \mid t = 1, ..., N\}$.

Задачу идентификации состояния ИБ устройства IoT можно представить следующим образом. Пусть Z – множество состояний устройства, C – множество классов состояний, содержащих как безопасные – нормальные состояния, где выполняются заранее предопределенные процессы с показателями, находящимися в норме, так и опасные, – аномальные состояния. в которых существуют отклонения от предполагаемых значений. Выбрана метрика расстояния между объектами $r(z, z')$. Имеется конечная обучающая выборка известных состояний $\{z_1, ..., z_l\} \in Z$, которую необходимо разбить на подмножества $c_0, c_1, ..., c_p$, по метрике расстояния r и найти алгоритм $a: Z \to C$, отражающий множество Z во множество C. Под метрикой будем понимать функцию или формулу, определяющую расстояние (евклидово) между любыми точками и классами в метрическом пространстве [10]. Таким образом, цель состоит в том, чтобы обработать информацию сторонних и внутренних источников, на основе которой производить идентификацию состояния ИБ устройства.

Особенностью устройств IoT является то, что они представляют из себя с вычислительной точки зрения устройства, не обладающие большими ресурсами с ограниченным набором выполняемых команд, что позволяет рассматривать и идентифицировать ограниченный набор состояний и их переходов. Процессы приема, обработки и передачи сообщений, внутренние ситуации, связанные с реализацией вычислительных алгоритмов, поступающие команды управления воздействуют на устройство IoT, характеризующееся переходными характеристики $h(t)$ и состоянием внешней среды $u(t)$. Получается динамическая система, которая имеет k входов и d выходов [11], где на вход подается управляющая команда и значения переменных внешней среды, определяющих состояние устройства, а на выходе элемента появляются сигналы $S(t)$ (например, показывающие загрузку ресурсов, а также акустические, электромагнитные и т. д.), регистрируемые различными датчиками. Получаемые по внешним каналам дан-

ные зависят от параметра шумовой составляющей $v(t)$, связанного со свойствами измерительного прибора, характеристик получаемого сигнала и т. д.

В общем случае модель состояния IoT-устройства на основе информации измеренных сигналов определяется следующим типом соотношений [12]:

$$\sum_{i=1}^{q}\sum_{j=1}^{d}\int_0^t u_i(t)h_{ij}(t-\tau)\,\mathrm{d}\,\tau = \sum_{j=1}^{d}\int_0^t f\left(s_j(t), v_j(t)\right), \quad (1)$$

где: q – количество каналов источников; h – переходные характеристики i-го канала для j-го регистрирующего, получаемые по каналу значения датчика; f – функция измеренных значений.

Идентификация состояния устройства IoT происходит на основе данных в дискретные моменты времени t_0, t_1, ..., t_n векторов числовых последовательностей, регистрируемых в процессе функционирования устройства. Значения $X(t)$ определяются дискретной функцией, отражающей данные от датчиков, содержащие смесь полезного сигнала $S(t)$ и шума, выраженного параметром $v(t)$:

$$X(t) = \mathrm{F}\left[S(t), v(t)\right], \quad (2)$$

где вектор X является результатом смешанных взаимно независимых сигналов $S(t)$, имеющих искажение шумовой составляющей $v(t)$.

Особенности процессов регистрации данных позволяют говорить о временном ряде в представлении вектора X.

Идентификация состояния реализуется путем обработки поступающих от устройств данных [13-14]. Анализируемые состояния, определяемые множествами временных рядов в различных ситуациях функционирования IoT-устройств, разделяются на два подмножества: безопасные, где выполняются заранее предопределенные процессы, и опасные, где имеются отклонения от параметров в заданных режимах работы. На основе обучающей выборки определяются начальные центроиды. Затем по мере поступления анализируемых значений происходит вычисление расстояния до ближайшего центра кластера, анализ и включение нового объекта в объединение однородных элементов и вычисление нового центроида с учетом обработанной информации. Векторы X_1, X_2, ..., X_n представляют числовые значения временных рядов, отражающие поведение процесса. На основе их значений определяется множество состояний Z. C – множество классов, где подмножества разделяются на опасные C_1 и безопасные C_2 состояния. Существует целевая зависимость – отображение $Z \to C$, значения которой известны только на объектах конечной обучающей выборки $X = \left\{(x_{11}, ..., x_{n1}), (x_{12}, ..., x_{n2}), ..., (x_{1m}, ..., x_{nm})\right\}$. Необходимо построить алгоритм обработки $X_i - a$, способный классифицировать подаваемый на вход вектор.

Над состояниями Z, которые характеризуются векторами синхронизированных временных рядов X, полученных от датчиков и сенсоров, проводится наблюдение. Определяется, к какому классу C и его подмножествам C_1, C_2 относится исследуемое состояние z_j. Значения векторов X, которые содержат

шаблонные последовательности от датчиков в различных условиях функционирования, отнесенных к классам множеств C_1, C_2, являются обучающей выборкой.

По очередным поступающим значениям синхронизированного временного ряда нескольких датчиков $x = (x_{1i}, ..., x_{ni})$ вектора признаков $X = X_1, X_2, ..., X_n$ проводится идентификация класса $\{C_i | i = 1,2\}$, соответствующего состоянию z_j. Распределения значений случайного вектора X имеют разные параметры.

Решающее правило $r'(x)$ для алгоритма a ставит в соответствие наблюдению x одно из множеств C_1 или C_2. Оно определяется функцией $f(x)$, порождающей разбиение пространства на две непересекающиеся области:

$$r'(x) = \begin{Bmatrix} C_1, & \text{при } f(x) \geq \varepsilon \\ C_2, & \text{при } f(x) < \varepsilon \end{Bmatrix}, \quad (3)$$

где ε – пороговое значение.

Предложенный подход идентификации состояния отличается использованием шаблонных последовательностей, описывающих сложившиеся в прошлом условия функционирования устройства, содержащих синхронизированные временные ряды, показывающие полученные от различных датчиков и сенсоров числовые значения во время выполнения процессов, что позволяет определять состояние ИБ, не увеличивая объема базы данных хранящейся информации.

Использование предлагаемого подхода на первоначальном этапе предполагает «настройку» устройства в заранее заданных режимах работы, где происходит предобработка, связанная с вычислением кластерных областей и пороговых значений, что может происходить на основе обучающей выборки. На этапе функционирования на основе функции разбиения пространства осуществляется соотнесение текущего состояния к определенным на первоначальном этапе.

Дальнейший анализ отклонений происходит на основе сравнений с эталонными значениями центров кластеров и классов, вычисленными в условиях, заданных при формировании обучающей выборки.

Результаты эксперимента

В рамках эксперимента по реализации предлагаемого подхода было выполнено соединение типа «сетевой мост». Схема проведения эксперимента приведена на рис. 1.

Для мониторинга состояния информационной безопасности обнаружение изменений вычислительной среды, процессов, реализующих функционал в интересах злоумышленника, является актуальным проблемным вопросом. В связи с этим возникает необходимость идентифицировать состояние функционирующего устройства как «безопасное» или «небезопасное».

Целью проведения эксперимента было выявление состояния, определяемого алгоритмом обработки данных, вычислительного узла на основе оцифрованных показателей загрузки вычислительных ресурсов [15-17]. В качестве последовательности, формирующей поведенческий паттерн, были выделены син-

хронизированные по времени процентные показатели монитора системной загрузки.

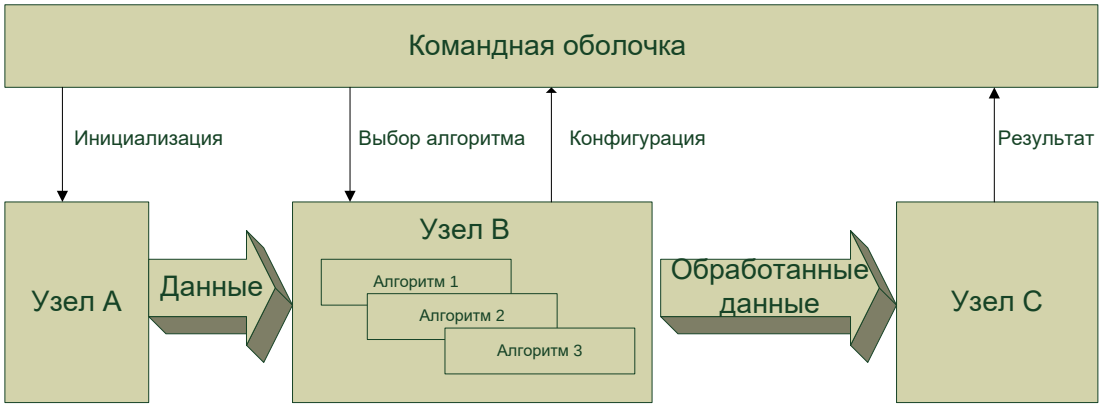


Рис. 1. Схема проведения эксперимента

От узла A на узел B через узел C передавались файлы, содержащие поля таблиц баз данных. На узле C происходило переключение алгоритмов обработки. В первом случае передача информации осуществлялась через узел C без обработки (состояние Z_1), во втором (состояние Z_2) – производилась фильтрация по заранее заданному полю таблицы, в третьем (состояние Z_3) – выполнялись вычисления и к передаваемой таблице добавлялись дополнительные поля. Условно считая, что Z_1 – безопасное состояние, а Z_2 и Z_3 – небезопасные, идентификация состояния ИБ определялось через сигнальные последовательности трасс системного монитора узла C.

Синхронизированные во времени последовательности значений процентного использования ресурсов центрального процессора, сетевых пакетов, потребляемых ресурсов памяти представлены в виде выходных векторов.

При проведении эксперимента была получена выборка паттернов сигнальных трасс для рассматриваемых состояний, которая была разделена на «обучающую» и «тестовую» (рис. 2-4).

Идентификация состояния выполнялась на основе метода кластеризации k-средних [18-19]. В качестве меры близости (4) использовано Евклидово расстояние:

$$r(x, \dot{x}) = \sqrt{\sum_{\rho=1}^{n} (x_\rho - \dot{x}_\rho)^2}\ , \tag{4}$$

где: R – пространство наблюдений; $x,\ \dot{x} \in R^n$.

С помощью значений обучающей выборки на основе метода k-средних произведено разделение (5) q наблюдений на l групп (или кластеров) $(l \le q),\ C = \{C_1,\ C_2,\ ...,\ C_0\}$:

$$\min \left[\sum_{i=1}^{l} \sum_{x} (C)_{\in z} \left| x^{(j)} - \mu_i \right|^2 \right], \tag{5}$$

где: $x^{(j)} \in R^n$; $\mu_i \in R^n$; μ_i – центроид для кластера C_i.

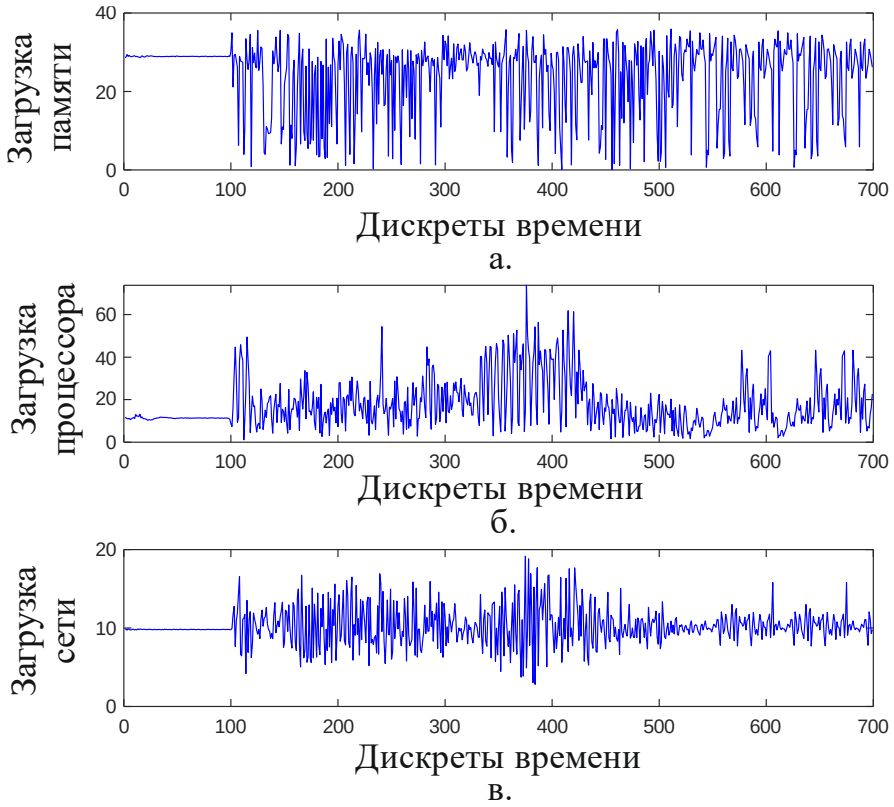


Рис. 2. Пример выборки процентной загрузки ресурсов (сверху вниз соответственно – память, процессор, сеть) от дискретов времени (временные отчеты от 0 до 600) для состояния z_1

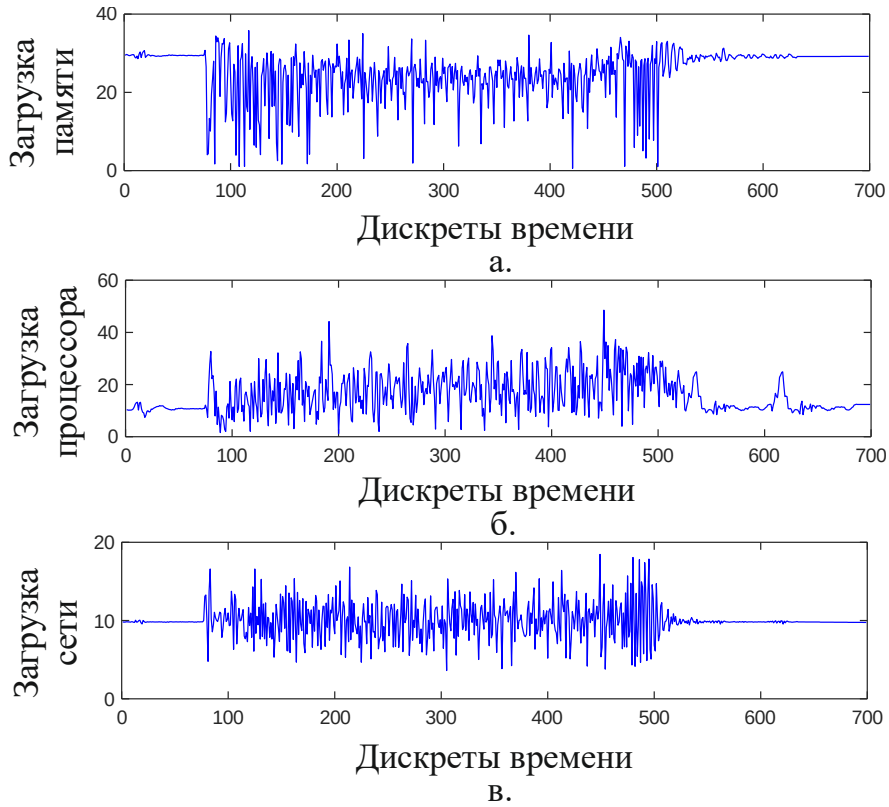


Рис. 3. Пример выборки процентной загрузки ресурсов (сверху вниз соответственно – память, процессор, сеть) от дискретов времени (временные отчеты от 0 до 600) для состояния z_2

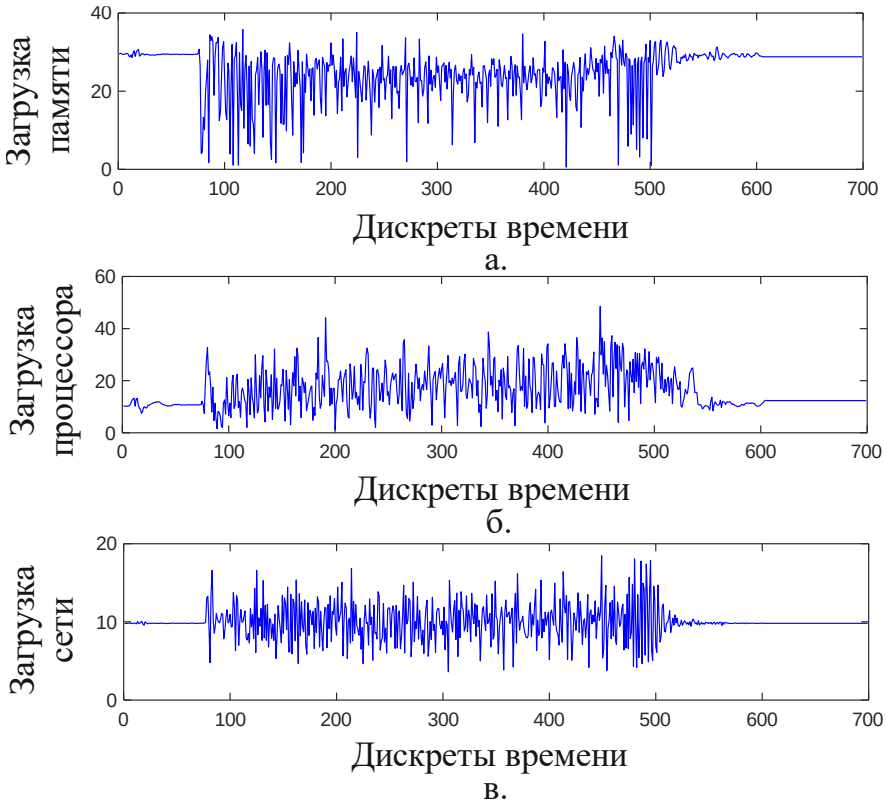


Рис. 4. Пример выборки процентной загрузки ресурсов (сверху вниз соответственно – память, процессор, сеть) от дискретов времени (временные отчеты от 0 до 600) для состояния Z_3

Процесс идентификации состояния заключался в том, что по данным поступающей последовательности вычисляются значения, которые сравниваются с центроидами кластеров.

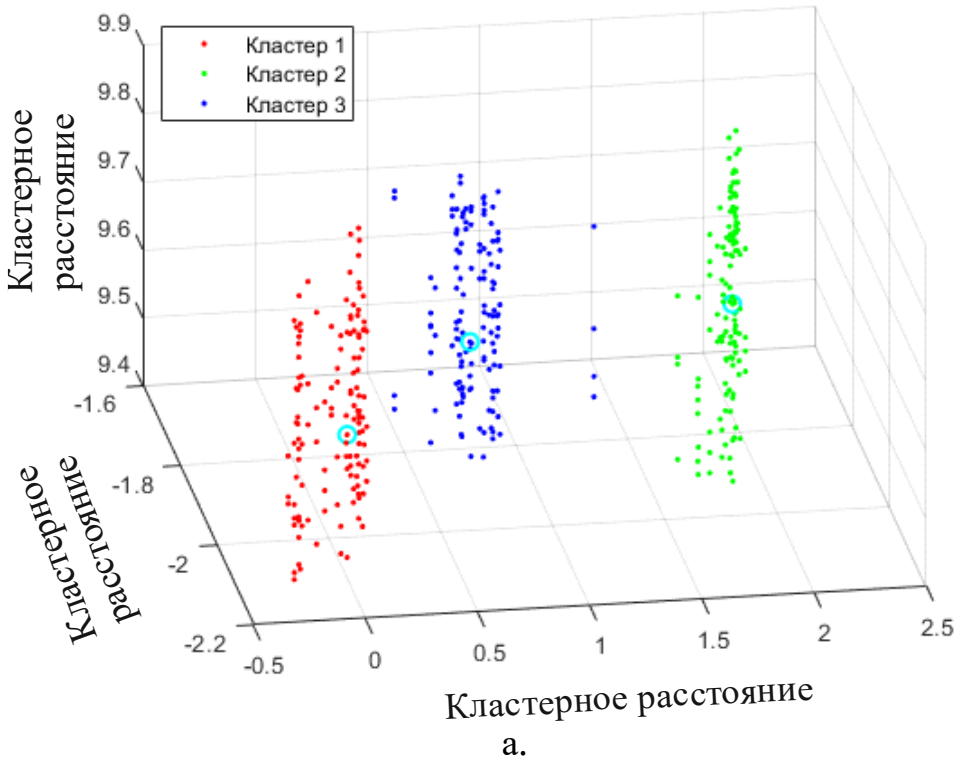
Фиксируемые временные ряды последовательностей значений от центрального процессора, сетевых пакетов, потребляемых ресурсов памяти для различных состояний, а также кластеры состояний достаточно хорошо отличаются друг от друга (выражения (4) и (5)), что визуально прослеживается на областях (рис. 5) и подтверждается анализом размеров кластеров и расстояний внутри (рис. 6).

Измеряя расстояние до центроидов, выбирается минимальное значение, на основе которого принимается решение о принадлежности к кластеру, идентифицирующему состояние. Общая точность выбранного предложенного решения для случая полной классификации составила 0,96 (рис. 6-7).

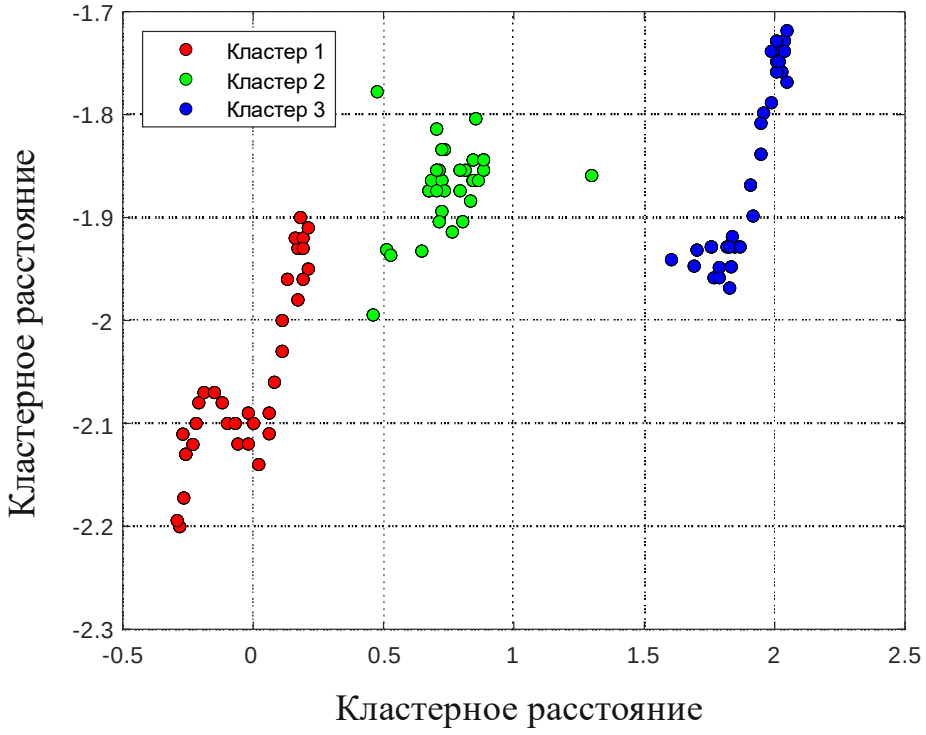
Гистограмма на рис. 6 показывает, что выбранные значения векторов, идентифицирующих состояние, разбиты на три кластера одинакового размера, что соответствует характеристикам экспериментальных выборок данных. Большинство точек в рассматриваемых кластерах имеют большие значения относительного расстояния (0,8 или более), что указывает на то, что кластеры хорошо разделены.

Для визуального анализа данных на рис. 7 полученные значения векторов отображены в виде матрицы двумерных декартовых графиков рассеяния, сгруппированных по различным входным аргументам. На основе отображае-

мых данных и их гистограмм можно определить качество признаков, влияющих на идентификацию состояний.



а.



б.

Рис. 5. Результаты кластеризации на основе среднего значения изменения координат

№3. 2020
ISSN 2410-9916

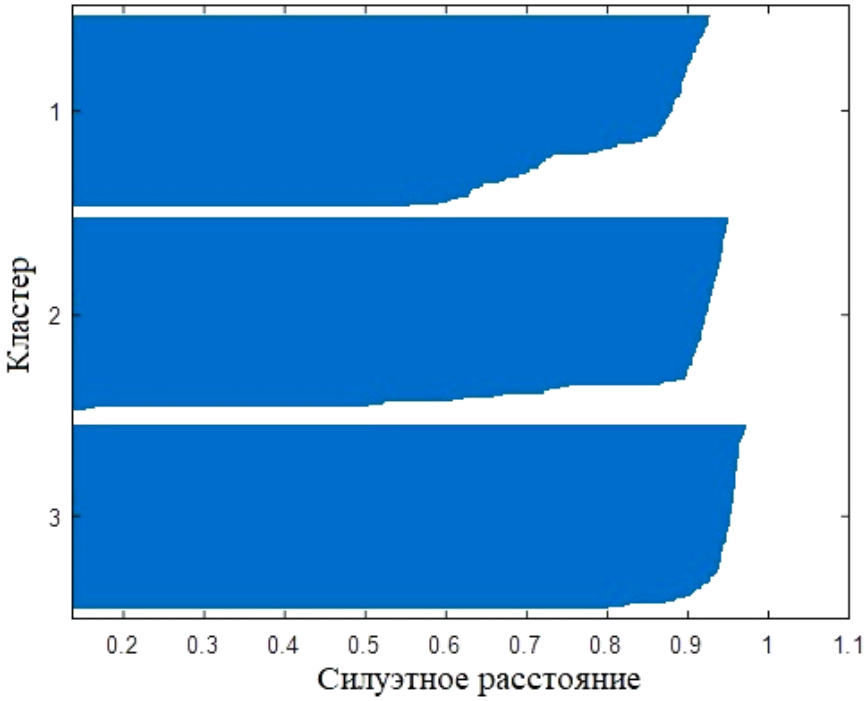


Рис. 6. Визуализация оценки полученных кластеров

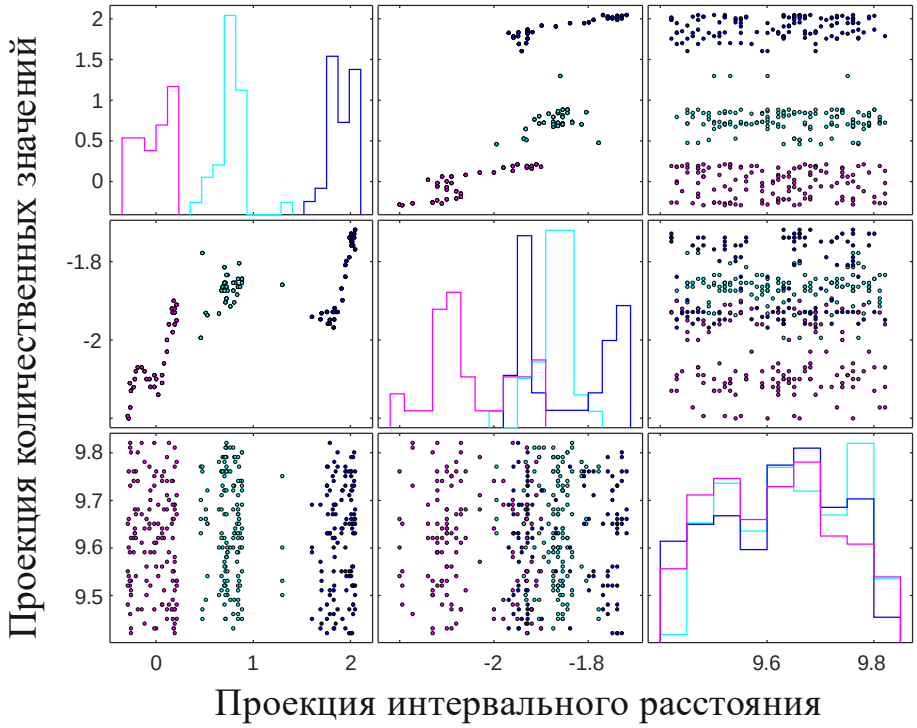


Рис. 7. Качество признаков (*строки сверху вниз* – загрузка памяти, процессора и сети), влияющих на идентификацию состояний

В проведенном вычислительном эксперименте видно, что наибольший вклад в качество идентификации состояния ИБ вносят сигналы, отражающие загрузку памяти.

Таким образом, предлагаемый подход позволяет определить класс текущего состояния.

DOI: 10.24411/2410-9916-2020-10310
URL: https://sccs.intelgr.com/archive/2020-03/10-Sukhoparov.pdf

В дальнейшем в качестве продолжения исследования, анализируя значения для различных задач оптимизации объема вычислений или базы данных, где хранятся синхронизированные временные ряды, полученные от датчиков и сенсоров, можно использовать аддитивный критерий, например обобщенный критерий оптимальности $\min_{\bar{x}\in X} F\left(\bar{w}, \bar{X}(t)\right) = \min_{\bar{x}\in X} \sum_{i=1}^{s} w_i X_i(t)$ при условии $\sum_{i=1}^{s} w_i = 1$, где w_i – весовые коэффициенты, что позволяет создавать приоритет более важным частным критериям за счет увеличения для них значений w_i.

Выводы

Процесс мониторинга состояния ИБ изменяющихся в динамике состояний устройств интернета вещей является трудоемким и требует анализа большого числа показателей. Выбор анализируемых данных оказывает существенное влияние на качественные показатели определения состояний. К ошибкам идентификации может приводить как недостаточное, так и избыточное количество информативных показателей.

Предлагаемый подход идентификации состояния ИБ устройства интернета вещей на основе метода k-средних позволяет определить текущее состояние. Он используется для предобработки информации временных рядов, полученной от регистрирующих устройств в различных режимах функционирования. Наличие заранее определенных обучающих выборок дает возможность исключить трудоемкие процессы вычисления параметров для режимов функционирования. Автоматически определяя характеристики кластеров и используя разбивающие пространство функции, становится возможным определять класс текущего состояния без существенных затрат вычислительных ресурсов.

Основным ограничением предложенного подхода является необходимость выбора синхронизированных временных рядов от датчиков и сенсоров. Другое ограничение, влияющее на качественные показатели применения метода, – выбор длин рассматриваемых интервалов. Правильное формирование обучающей выборки оказывает существенное влияние на дальнейшие результаты метода, а это требует анализа возможных фоновых закономерностей, наличия достаточного количества классифицируемых последовательностей, анализа разбалансировки и корреляции последовательностей. Частичное решение подобных проблемных вопросов может быть реализовано с помощью увеличения объемов выборки. Комбинирование характеристик может позволить повысить точность оценки состояния устройства, но требует дополнительных исследований.

Другим направлением развития подобных решений, учитывая относительную ограниченность ресурсов устройств IoT, является организация внешних центров обработки данных, на которые устройства интернета вещей могут отправлять информацию о своем функционировании для дальнейшего анализа состояния.

Основным достоинством предложенного подхода является относительная простота его реализации и минимальные требования к вычислительным ресурсам. Предложенный подход идентификации состояния ИБ IoT-устройств отличается от известных [1-3, 5, 14-15] применением шаблонных последовательностей, описывающих сложившиеся в прошлом условия функционирования устройства, содержащих синхронизированные временные ряды, показывающие полученные от различных датчиков и сенсоров числовые значения во время выполнения процессов, что позволяет определять состояние ИБ, не увеличивая объема базы данных хранящейся информации.

Литература

1. Farwell J. P., Rohozinski R. Stuxnet and the Future of Cyber War // Survival. 2011. Vol. 53. № 9. P. 23-40. doi: 10.1080/00396338.2011.555586.

2. Yeung D. Y., Ding Y. Host-based intrusion detection using dynamic and static behavioral models // Pattern recognition. 2003. Vol. 36. P. 229-243. doi: 10.1016/S0031-3203(02)00026-2.

3. Igure V., Laughter S., Williams R. Security issues in SCADA networks // Computers & Security. 2006. Vol. 25. № 7. P. 498-506. doi: 10.1016/j.cose.2006.03.001.

4. 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.

5. 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. № 2. P. 96-110. DOI: 10.1109/TDSC.2008.39.

6. Макаренко С. И., Олейников А. Я, Черницкая Т. Е. Модели интероперабельности информационных систем // Системы управления, связи и безопасности. 2019. № 4. С. 215-245.

7. 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. DOI: 10.1088/0022-3727/14/3/007.

8. 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. DOI: 10.1007/978-3-030-30859-9_9.

9. 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. № 1. С. 98-105.

10. Сошникова Л. А., Тамашевич В. Н., Усбе Г., Шефер М. Многомерный статистический анализ в экономике: учебное пособие для вузов. – М.: ЮНИТИ – Дана, 1999. 598 с.

11. 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.

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

13. 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.

14. Lockhart D. J. Expression monitoring by hybridization to high-density oligonucleotide arrays // Natural Biotechnol. 1996. Vol. 14. P. 1675-1680. DOI: 10.1038/nbt1296-1675.

15. Golub T. R. Molecular classification of cancer: class discovery and class prediction by gene expression monitoring // Science. 1999. Vol. 286. P. 531-537. DOI: 10.1126/science.286.5439.531.

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

17. Dembele D., Kastner P. Fuzzy C-means method for clustering microarray data // Bioinformatics. 2003. Vol. 19. № 8. P. 973-980. doi: 10.1093/bioinformatics/btg119.

18. Rousseeuw J. P. Silhouettes: a graphical aid to the interpretation and validation of cluster analysis // Journal of Computational and Applied Mathematics. 1987. Vol. 20. P. 53-65. DOI: 10.1016/0377-0427(87)90125-7.

19. Whitfield M. L. Identification of Genes Periodically Expressed in the Human Cell Cycle and Their Expression in Tumors // Molecular Biology of the Cell. 2002. Vol. 13. № 6. P. 1977-2000. DOI: 10.1091/MBC.02-02-0030.

References

1. Farwell J. P., Rohozinski R. Stuxnet and the Future of Cyber War. *Survival*, 2011, vol. 53, no. 9, pp. 23-40. doi: 10.1080/00396338.2011.555586.

2. Yeung D. Y., Ding Y. Host-based intrusion detection using dynamic and static behavioral models. *Pattern recognition*, 2003, vol. 36, pp. 229-243. DOI: 10.1016/S0031-3203(02)00026-2.

3. Igure V., Laughter S., Williams R. Security issues in SCADA network. *Computers & Security*, 2006, vol. 25, no. 7, pp. 498-506. DOI: 10.1016/j.cose.2006.03.001.

4. Zikratov I. A., Zikratova T. V., Lebedev I. S. Doveritel'naya model' informacionnoj bezopasnosti mul'tiagentnyh robototekhnicheskih sistem s decentralizovannym upravleniem [A trust model of information security of multi-agent robotic systems with decentralized control]. *Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*, 2014, vol. 2, pp. 47-52 (in Russian).

5. 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. DOI: 10.1109/TDSC.2008.39.

6. Makarenko S. I., Oleynikov A. Y., Chernitskaya T. E. Modeli interoperabel'nosti informacionnyh sistem [Models of interoperability assessment for information systems]. *Systems of Control, Communication and Security*, 2019, vol. 4, pp. 215-245 (in Russian).

7. 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, no. 3, pp. 373-388. DOI: 10.1088/0022-3727/14/3/007.

8. 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. DOI: 10.1007/978-3-030-30859-9_9.

9. Lebedev I. S., Semenov V. V., Sukhoparov M. E. Podhod k klassifikacii sostoyaniya informacionnoj bezopasnosti elementov kiberfizicheskih sistem s ispol'zovaniem pobochnogo elektromagnitnogo izlucheniya [Approach to the classification of information security status of elements of cyberphysical systems using spurious electromagnetic radiation]. *Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 1, pp. 98-105 (in Russian).

10. Soshnikova L. A., Tamashevich V. N., Usbe G., Shefer M. *Mnogomernyj statisticheskij analiz v ekonomike* [Multivariate statistical analysis in economics]. Moscow, UNITI-Dana, 1999, 598 p. (in Russian).

11. Sukhoparov M. E., Lebedev I. S, Semenov V. V., Salakhutdinova K. I. Vyyavlenie anomal'nogo funkcionirovaniya ustrojstv industrii 4.0 na osnove povedencheskih patternov [Identification of the abnormal functioning of «Industry 4.0» devices based on behavioral patterns]. *Information Security Issues. Computer systems*, 2020, vol. 41, no. 1, pp. 96-102 (in Russian).

12. Bendat D., Piersol A. *Primenenie korrelyacionnogo i spektral'nogo analiza* [Engineering applications of correlation and spectral analysis]. Wiley, New York, 1980, 324 p. (in Russian).

13. Zasov V. A., Tarabardin E. N., Nikonorov E. N. Algoritmy i ustrojstva dlya identifikacii vhodnyh signalov v zadachah kontrolya i diagnostiki dinamicheskih ob"ektov [Algorithms and devices for identifying input signals in the tasks of monitoring and diagnostics of dynamic objects]. *Bulletin of the Samara State Aerospace University*, 2009, vol. 2, p. 115-123 (in Russian).

14. Lockhart D. J. Expression monitoring by hybridization to high-density oligonucleotide arrays. Natural Biotechnol, 1996, vol. 14, pp. 1675-1680. DOI: 10.1038/nbt1296-1675.

15. Golub T. R. Molecular classification of cancer: class discovery and class prediction by gene expression monitoring. *Science*, 1999, vol. 286, pp. 531-537. DOI: 10.1126/science.286.5439.531.

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

17. Dembele D., Kastner P. Fuzzy C-means method for clustering microarray data. *Bioinformatics*, 2003, vol. 19, no. 8, pp. 973-980. DOI: 10.1093/bioinformatics/btg119.

18. Rousseeuw J. P. Silhouettes: a graphical aid to the interpretation and validation of cluster analysis. *Journal of Computational and Applied Mathematics*, 1987, vol. 20, pp. 53-65. DOI: 10.1016/0377-0427(87)90125-7.

19. Whitfield M. L. Identification of Genes Periodically Expressed in the Human Cell Cycle and Their Expression in Tumors. *Molecular Biology of the Cell*, 2002, vol. 13, no. 6, pp. 1977-2000. DOI: 10.1091/MBC.02-02-0030.

Статья поступила 06 июля 2020 г.

Информация об авторах

Сухопаров Михаил Евгеньевич – кандидат технических наук. Старший научный сотрудник. Санкт-Петербургский филиал Акционерного общества «НПК «ТРИСТАН». Область научных интересов: безопасность сетевых технологий, сетей, телекоммуникаций. E-mail: sukhoparovm@gmail.com

Адрес: 195220, Россия, г. Санкт-Петербург, пр. Непокоренных, д. 47.

Лебедев Илья Сергеевич – доктор технических наук, профессор. Заведующий лабораторией интеллектуальных систем. Санкт-Петербургский Федеральный исследовательский центр Российской академии наук. Область научных интересов: безопасность сетевых технологий, сетей, телекоммуникаций. E-mail: isl_box@mail.ru

Адрес: 199178, Россия, г. Санкт-Петербург, 14 линия В.О., д. 39.

Identification the Information Security Status for the Internet of Things Devices in Information and Telecommunication Systems

M. E. Sukhoparov, I. S. Lebedev

Problem statement: *The development of information, technological, and cyber-physical systems is associated with the Internet of Things. Therefore, there is a need to develop models for ensuring information security, operability, stability of functioning, and methods aimed at lessons learned of various threats. Typical information security monitoring systems show are mostly embedded. Such solutions have certain disadvantages when withstanding exploits, logical bombs, and virus infections. Often the analyzed device is located outside the controlled area or is difficult to access. Thus, the processes occurring in devices and Internet of Things nodes must be subject to constant monitoring to ensure operability, stability, functionality, and information security.* ***The main objective of the study*** *is the additional information from external independent sources, calculated based on external channels, used to identify the associated characteristics of Internet of Things devices' state. This requires identifying the state based on time-synchronized tuples of signs.* ***The proposed approach:*** *The environment and various internal situations related to the processes of computing, messaging, competing for resources, and communication channels affect Internet of Things elements. The sequence of control commands received by the device determine the internal situations. External environment introduces a number of effects associated with temporary, physical resource constraints and interference. The authors propose to have the process of monitoring the information security state be carried out based on the k-means method. This implements decision-making using behavioral patterns and digitized signal paths patterns obtained during the operation of various system nodes. The calculation of the information security state of an Internet of Things device is implemented by comparing the behavioral patterns of the*

*digitized signal paths to the reference values obtained under "normal functioning". **Methods used:** solution of the problem is based on clustering methods, classification methods. Elements of statistical analysis methods are also applied. **The novelty** is in applying behavioral patterns to the digitized values of signal paths received from various external independent sources. **Key results:** an approach to identifying the state of information security of an Internet of Things device in the context of limited computing resources. **Practical relevance:** proposed approach makes it possible to identify the state of information security of an Internet of Things device without increasing the amount of information stored and processed in internal resources.*

Key words: *state analysis, behavioral patterns, nodes and devices of the Internet of things, network infrastructure, cyber-physical systems.*

Information about Authors

Mikhail Evgenievich Sukhoparov – Ph.D. of Engineering Sciences. Senior Researcher. St. Petersburg branch Joint Stock Company «NPK «TRISTAN». Field of Research: Security of Network Technologies, Networks, Telecommunications. E-mail: sukhoparovm@gmail.com

Address: Russia, 195220, Saint-Petersburg, Nepokorennykh prospect, 47.

Ilya Sergeevich Lebedev – Dr. habil. of Engineering Sciences, Full Professor. Head of Intelligent Systems Laboratory. St. Petersburg Institute of Informatics and Automation of the Russian Academy of Sciences. Field of Research: Security of Network Technologies, Networks, Telecommunications. E-mail: isl_box@mail.ru

Address: Russia, 199178, Saint-Petersburg, 14th Line V.O., 39.