НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2022 Том 22 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2022 Vol. 22 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2022-22-6-1150-1158
УДК 004.021

Метод мониторинга состояния элементов киберфизических систем на основе анализа временных рядов

Виктор Викторович Семенов✉

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, 199178, Российская Федерация

v.semenov@spcras.ru✉, https://orcid.org/0000-0002-7216-769X

Аннотация

Предмет исследования. Широкое распространение киберфизических систем, а также повсеместная интеграция вычислительных ресурсов в физические сущности привели к повышению рисков преднамеренных и случайных инцидентов безопасности. В связи с этим приобретает особую актуальность разработка новых и совершенствование существующих методов и средств мониторинга таких систем. Создаваемые и модернизируемые методы должны обладать повышенной полнотой и точностью идентификации, в особенности для объектов критической инфраструктуры. **Метод.** Предложен оригинальный метод обработки данных мониторинга состояния киберфизических систем на основе анализа временных рядов с применением весовых коэффициентов значимости в качестве постобработки результатов классификации. Метод отличается от существующих комбинированным подходом, сочетающим применение в системах мониторинга событий информационной и функциональной безопасности. Характеризуется использованием ансамбля деревьев решений, а также параллельно работающих классификаторов и весовых коэффициентов Фишберна при анализе совокупности наиболее информативных признаков, полученных из временных рядов. **Основные результаты.** Применимость метода обоснована при помощи вычислительного эксперимента на известном наборе данных, характеризующем функционирование информационной и физической составляющих при осуществлении различных типов атак на компоненты экспериментального стенда киберфизической системы водоочистки. Точность идентификации по сравнению с лучшими подходами, представленными в научных работах при использовании разработанного метода, увеличилась на 1,45 %, полнота — на 4,45 % и составила 99,85 % для обоих показателей. **Практическая значимость.** Полученные результаты адаптированы для практического использования в системах идентификации состояния киберфизических систем. Теоретическая значимость состоит в возможности использования результатов исследования при проектировании систем мониторинга информационной и функциональной безопасности киберфизических систем.

Ключевые слова

системы мониторинга, анализ временных рядов, киберфизические системы, выявление аномалий, информационная безопасность, функциональная безопасность, решающие деревья

Ссылка для цитирования: Семенов В.В. Метод мониторинга состояния элементов киберфизических систем на основе анализа временных рядов // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 6. С. 1150–1158. doi: 10.17586/2226-1494-2022-22-6-1150-1158

Method for monitoring the state of elements of cyber-physical systems based on time series analysis

Viktor V. Semenov✉

St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg, 199178, Russian Federation

v.semenov@spcras.ru✉, https://orcid.org/0000-0002-7216-769X

Abstract

The wide spread of cyber-physical systems, as well as the widespread integration of computing resources into physical entities, have led to an increase in the risks of deliberate and accidental security incidents. In this regard, the development

of new methods and tools and improvement of the existing ones for monitoring such systems is of particular relevance. The methods being created and modernized should have increased recall and precision of identification, especially for critical infrastructure objects. An original method for processing data for monitoring the state of cyber-physical systems based on time series analysis using significance weights as a post-processing of classification results was proposed. The method differs from the existing ones by the combined approach that combines the use events of information security and functional safety in monitoring systems. It is characterized by the use of an ensemble of decision trees as well as parallel classifiers and Fishburn weight coefficients in the analysis of the set of the most informative features obtained from time series. The applicability of the method was substantiated by conducting of a computational experiment on a known data set which characterizes the functioning of the information and physical components in the implementation of various types of attacks on the components of the experimental stand of the cyber-physical water treatment system. When using the developed method, the identification precision increased by 1.45 % compared to the best approaches presented in other scientific works, and the recall increased by 4.45 % and amounted to 99.85 % for both indicators. The results obtained are adapted for practical use in systems for identifying the state of cyber-physical systems. The theoretical significance lies in the possibility of using the results of the study in the design of systems for monitoring the information security and functional safety of cyber-physical systems.

Keywords
monitoring systems, time series analysis, cyber-physical systems, identification of anomalies, information security, functional safety, decision trees

For citation: Semenov V.V. Method for monitoring the state of elements of cyber-physical systems based on time series analysis. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 6, pp. 1150–1158 (in Russian). doi: 10.17586/2226-1494-2022-22-6-1150-1158

Введение

Слияние информационных технологий и промышленных процессов, наблюдаемое в последние годы в развитии технологической инфраструктуры, привело к трансформации принципов построения производственных объектов и широкому распространению киберфизических систем (КФС).

На современном этапе развития КФС отмечается повышение степени интеллектуальности систем управления, их автономности и адаптивности, вместе с этим стремительно возрастает объем обрабатываемой информации, передаваемой от различных сенсоров и датчиков [1]. Данные системы являются сложными и распределенными, что также ведет к возникновению ряда проблем, связанных с их работоспособностью и информационной безопасностью (ИБ) [2]. Таким образом, необходимо обеспечение постоянного мониторинга состояния КФС, в том числе оценки защищенности, при этом крайне важным является учет временных параметров потенциальных инцидентов безопасности.

Среди основных уязвимостей КФС можно выделить: возможность прослушивания каналов, посылку «внешних» пакетов, осуществление физического доступа злоумышленника к объекту КФС, недостаточную стандартизацию интеллектуальных алгоритмов маршрутизации, учитывающих состояние сети и др. На рис. 1 приведены типовые деструктивные воздействия

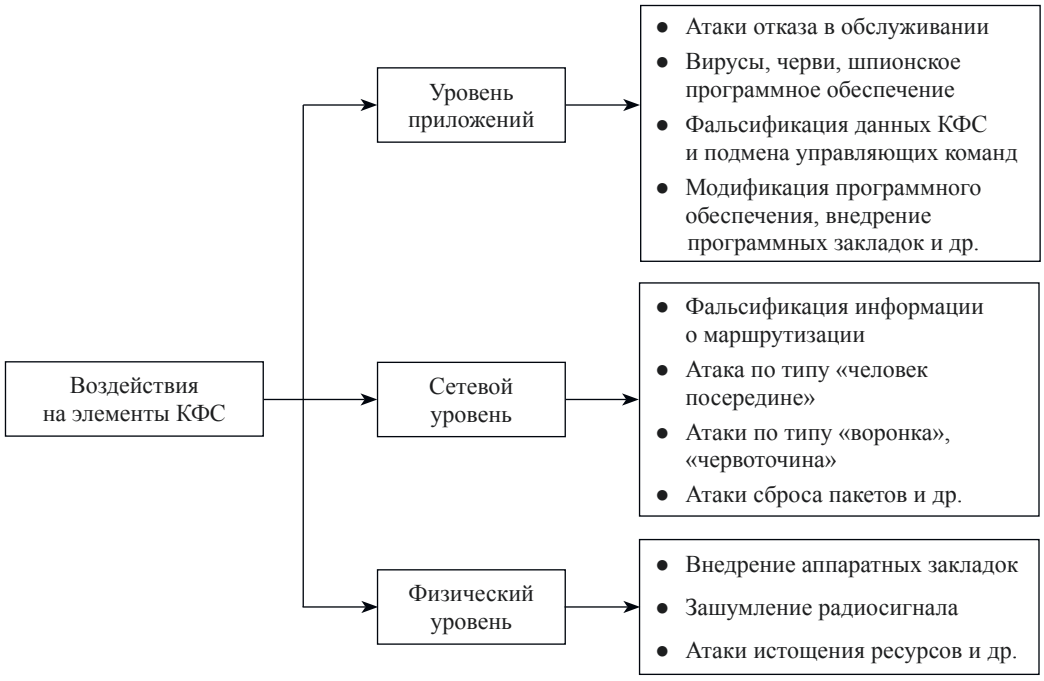

Рис. 1. Угрозы безопасности на различных уровнях киберфизических систем
Fig. 1. Security threats at different levels of the cyber-physical systems

на элементы КФС на различных уровнях: физическом, сетевом и уровне приложений.

Управление инцидентами безопасности, включая их выявление, фиксацию, предсказание — постоянный сложный процесс наблюдения и анализа результатов событий безопасности и иных данных. Подобного рода мониторинг представляет собой комплексную задачу по работе с угрозами и нарушениями ИБ, а также технологическими сбоями и отказами, осложненными разнородностью промышленных сетевых устройств и протоколов, количеством данных и скоростью их поступления. Дополнительную проблему предоставляет необходимость адаптации средств мониторинга в динамически меняющихся условиях. Исходя из этого, перспективной задачей является разработка методов мониторинга состояния элементов КФС с целью обеспечения их комплексной информационно-функциональной безопасности, а также устойчивого функционирования в условиях наличия информационных угроз и атак.

Существующие методы и технологии в большей мере ориентированы на классические компьютерные или информационные системы [3–5], что ограничивает возможность их применения в КФС. Используемые на сегодняшний день решения [6, 7] не обладают достаточным функционалом, обеспечивающим эффективный мониторинг в режиме реального времени, что вызывает ряд проблем обеспечения информационно-функциональной безопасности, связанных с анализом состояния отдельных устройств КФС. В связи с этим возникает объективная необходимость развития и адаптации методов математического обеспечения специализированных информационных систем, интегрируемых в КФС, в целях противодействия внешним и внутренним деструктивным воздействиям.

Настоящая работа — логическое продолжение работ [8, 9].

Постановка задачи

Рассмотрим задачу классификации временных рядов, характеризующих состояние информационно-функциональной безопасности КФС. Пусть имеется временной ряд $\mathbf{X} = \{\{x_1(t_1), x_2(t_1), \ldots, x_S(t_1)\}, \{x_1(t_2), x_2(t_2), \ldots, x_S(t_2)\}, \ldots, \{x_1(t_m), x_2(t_m), \ldots, x_S(t_m)\}\}$, каждому кортежу которого соответствует набор характеристик информационных или физических процессов КФС в дискретный момент времени; $\{c_1, \ldots, c_l\}$ — множество состояний КФС, l — число идентифицируемых состояний КФС; $C = \{C_0, C_1\}$ — множество рассматриваемых состояний. Каждый элемент КФС может находиться в опасном (C_1) или безопасном (разрешенном) (C_0) состоянии. $C_0 = \{c_1, c_2, \ldots, c_k\}$, $C_1 = \{c_{k+1}, c_{k+2}, \ldots, c_l\}$, k — число безопасных состояний КФС.

Требуется определить состояние КФС (метка класса c), к которому относится подаваемый на вход элемент временного ряда. Для обучения модели необходимо получить характеристику протекающих информационных и физических процессов каждого рассматриваемого состояния КФС. Формирование обучающей выборки может производиться, например, с использованием программного обеспечения для автоматизированного анализа сетевого трафика.

Метка класса состояния КФС c в дискретный момент времени t описывается с использованием предлагаемого в работе метода при помощи ряда отобранных согласно работе [8] наиболее информативных признаков:

$$c = \mu(a_1(x_{t,1}, x_{t,2}, \ldots, x_{t,s}), a_2(x_{t,1}, x_{t,2}, \ldots, x_{t,s}), \ldots, a_n(x_{t,1}, x_{t,2}, \ldots, x_{t,s})),$$
$$c \in C, x_{t,i} \in D_f, s << S,$$

где C — множество рассматриваемых состояний КФС; μ — агрегирующая функция; a_1, a_2, …, a_n — классифицирующие алгоритмы; $x_{t,i}$ — значения признаков в дискретный момент времени; D_f — множество допустимых значений признаков; s — количество отобранных наиболее информативных признаков; S — общее количество доступных признаков.

Цель работы — разработка метода, обеспечивающего увеличение полноты и точности идентификации состояния информационно-функциональной безопасности КФС за счет использования в системе мониторинга значений временных рядов за предшествующие моменты времени с применением весовых коэффициентов значимости.

Метод решения поставленной задачи

В работе применен и исследован алгоритм на основе деревьев решений, который относится к группе логических классификаторов [10]. Суть алгоритма заключается в построении бинарного дерева, во внутренних узлах которого располагаются предикаты, а в листах — метки классов c_i ($i = 1, \ldots, l$). Корень деревьев решений содержит узел принятия решения на основе анализа наиболее информативного признака, по мере удаления и при дальнейшем построении деревьев решений используются менее информативные признаки (по убыванию информативности). Листовые вершины содержат значения классов, определенных на этапе формирования обучающей выборки. Выбор предикатов осуществлен с помощью критериев информативности [11].

В бинарном дереве решений:

— каждой внутренней вершине v приписана функция (или предикат) β_v: $\mathbf{X} \to \{0, 1\}$;

— каждой листовой вершине v приписан прогноз — одно из l возможных состояний КФС $c_i \in C$.

Предикаты β_v сравнивают значение одного из признаков с порогом τ_v:

$$\beta_v(x; j, \tau_v) = [x_j < \tau_v].$$

Алгоритм $a(x)$, начиная с корневой вершины v_0, вычисляет значение функции β_{v0}. Если оно равно нулю, то алгоритм переходит в левую дочернюю вершину, иначе в правую, после чего вычисляет значение предиката в новой вершине и делает переход или влево, или вправо. Процесс продолжается, пока не будет достигнута листовая вершина; алгоритм возвращает тот класс, который приписан этой вершине.

Таким образом, подавая на вход исходные значения в момент времени t, построенный алгоритм $a(x)$ на основе обучающего набора формирует ответ — одну из меток класса $c_i \in C$, ассоциированную с состоянием КФС.

КФС — сложная система, каждый элемент которой может подвергаться отдельным видам деструктивных воздействий и атак. Данные, поступающие от различных элементов КФС, могут обладать индивидуальными свойствами. В связи с этим возникает задача идентификации состояния для классификаторов, обладающих своими компетенциями на подвыборках.

Временной ряд $\mathbf{X}$ состоит из значений признаков в m моментов. По методу бутстрэпа (bootstrap) из всего множества равновероятно выбирается m/n векторов признаков, каждый из которых соответствует определенному моменту времени. Отметим, что из-за возвращения некоторые элементы в подмножествах могут повторяться. Обозначим новую выборку через $\mathbf{X}_1$. Повторяя процедуру n раз, сгенерируем n подвыборок $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_n$.

Применим n параллельно работающих классификаторов для увеличения скорости получения итоговых результатов. Используем агрегирующую функцию μ для улучшения стабильности и точности алгоритмов. Принципы построения ансамбля параллельно работающих классификаторов:

— генерация с помощью бутстрэпа n выборок размерностью $m/n \times s$ для каждого классификатора a_1–a_n;
— независимое обучение каждого элементарного классификатора (алгоритм a_1–a_n, определенный на своем подпространстве) на заранее размеченном наборе данных (обучение с учителем);
— независимая классификация каждой подвыборки $\mathbf{X}_1$, $\mathbf{X}_2, \ldots, \mathbf{X}_n$ на каждом из подпространств;
— принятие окончательного решения о принадлежности объекта одному из состояний.

В классических подходах при использовании ансамблей классификаторов окончательное решение о принадлежности элементов временного ряда определенному состоянию КФС принимается одним из следующих методов.

— Консенсус: если все элементарные классификаторы присвоили одну и ту же метку множеству значений признаков в момент времени t, то такой объект будет отнесен к выбранному классу. Консенсус достижим не всегда.
— Простое большинство: объекту присваивается метка того класса, который определило для него большинство элементарных классификаторов.

При использовании «моментальных снимков» в дискретный момент времени не всегда достигается необходимая полнота и точность идентификации состояния КФС. Кроме того, на практике наиболее важными являются значения состояний, которые приближены к текущему моменту времени [9]. Для увеличения полноты и точности предлагается ввести временной отрезок идентификации N, представляющий собой скользящее окно от t_{i-N+1} до текущего момента времени t_i, и весовые коэффициенты p_i, учитывающие степень предпочтения одних результатов идентификации другим (рис. 2).

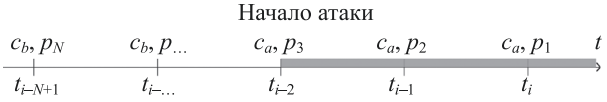

Рис. 2. Временной график идентификации атаки с учетом коэффициентов значимости

Fig. 2. Time schedule of attack identification which takes into account the coefficients of significance

В рассматриваемом случае c_b — безопасное состояние КФС; c_a — состояние, в котором КФС находится под атакующим информационным или физическим воздействием. Весовые коэффициенты должны удовлетворять следующим требованиям:

— учитывать временной отрезок идентификации N, представляющий собой значение величины временного интервала, за который анализируемые данные подаются на вход алгоритма, реализующего предложенный метод;
— любой коэффициент p_{i+1} должен быть меньше p_i ($\forall\, p_{i-1} < p_i$, $i \in [1, N]$).

Для системы убывающего предпочтения, состоящей из N альтернатив, предложено использовать весовые коэффициенты, снижающиеся по правилу арифметической прогрессии. Весовые коэффициенты Фишберна — рациональные дроби, в числителе которых расположены убывающие на единицу элементы натурального ряда от N до 1, а в знаменателе — сумма арифметической прогрессии N первых членов натурального ряда с шагом 1.

$$r_1 = N,\ r_i = r_{i-1} - 1,\ K = \sum_{i=1}^{N} r_i,\ p_i = \frac{r_i}{K}, \qquad (1)$$

где r_i — элементы натурального ряда; K — сумма арифметической прогрессии N первых членов натурального ряда с шагом 1; p_i — весовой коэффициент значимости результата идентификации для дискретного момента времени; N — временной отрезок идентификации.

Апробация метода

С целью практической реализации разработанного метода идентификации состояния элементов КФС на основе анализа временных рядов выполним расчетный эксперимент над набором данных [12]. Исследователи из Сингапурского университета технологии и дизайна (Singapore University of Technology and Design) смоделировали различные типы атак на компоненты экспериментального стенда КФС водоочистки. Для исследования выбраны атаки, которые происходили: на разных уровнях КФС; включали в себя один или несколько этапов; имели различную продолжительность и затрагивали разные уровни КФС; большинство атак имели воздействие на технологический процесс.

В табл. 1 представлены типы и количество атак (общее количество — 41).

Из полученного сетевого трафика между системой SCADA (Supervisory Control And Data Acquisition) и программируемыми логическими контроллерами сформированы временные ряды, содержащие информацию со всех доступных датчиков КФС. Для анализа вре-

Таблица 1. Типы атак на киберфизические системы водоочистки

Table 1. Types of attacks on cyber-physical systems of water treatment

Типы атак	Количество атак
Одностадийные и однонаправленные	26
Одностадийные многонаправленные	4
Многостадийные однонаправленные	2
Многостадийные и многонаправленные	4
Без воздействия на технологический процесс	5

менных рядов, характеризующих функционирование КФС, применено программное обеспечение MATLAB R2022a. Формирование деревьев решений, их ансамблей и последующая классификация выполнена при помощи приложения Classification Learner App.

Исходные данные для реализации разработанного метода представляют численный двумерный массив 944 919 × 51. В строках расположены значения временного ряда, регистрируемые раз в секунду, а столбцы упорядочены по источникам получения информации от КФС. Набор данных размечен по классам (состояниям), каждому временному ряду поставлена в соответствие метка класса $\{c_1, \ldots, c_{41}\}$.

В начале процесса оценивания состояния элементов КФС формируется обучающая выборка из временных рядов, составленных из значений параметров функционирования КФС и соответствующих им меток состояний (классов). Методом равномерного случайного сэмплинга с возвратом формируется n подвыборок.

Алгоритмы a_1–a_n на основе деревьев решений обучаются каждый на своей подвыборке независимо друг от друга, классификаторы не исправляют ошибки друг друга, а компенсируют их при голосовании. Базовые классификаторы в таком случае являются независимыми за счет обучения на различных подвыборках. На стадии идентификации состояния анализируемые показатели за отрезок времени N, представляющие собой кортеж $\mathbf{X}^* = \{\{x_1(t_{i-N+1}), x_2(t_{i-N+1}), \ldots, x_s(t_{i-N+1})\}, \ldots, \{x_1(t_{i-1}), x_2(t_{i-1}), \ldots, x_s(t_{i-1})\}, \{x_1(t_i), x_2(t_i), \ldots, x_s(t_i)\}\}$, подаются на вход вышеуказанных классифицирующих алгоритмов.

Каждый алгоритм a_1–a_n генерирует N ответов на заданном временном отрезке, которые постобрабатываются на первом этапе с использованием весовых коэффициентов Фишберна, придающих больший вес более поздним результатам идентификации. Таким образом, метка класса определяется путем взвешенного обобщения результатов классификации на отрезке времени N. Весовые коэффициенты p_i для различных моментов времени суммируются в том случае, если предсказанные классы совпадают. В табл. 2 приведен пример применения рассчитанных по формуле (1) коэффициентов для классификатора a_1.

Сумма коэффициентов для c_{37} равна $\frac{5}{15}$, c_{35} — $\frac{7}{15}$, c_{18} — $\frac{3}{15}$. С учетом весовых коэффициентов значимости результатом будет метка класса c_{35}. В случае равенства коэффициентов перед классами выберем тот класс, который был определен для более позднего момента времени.

Таблица 2. Пример применения весовых коэффициентов для $N = 5$

Table 2. An example of applying weigh coefficients for $N = 5$

Время	Весовой коэффициент	Метка класса состояния
t_i	$\frac{5}{15}$	c_{37}
t_{i-1}	$\frac{4}{15}$	c_{35}
t_{i-2}	$\frac{3}{15}$	c_{35}
t_{i-3}	$\frac{2}{15}$	c_{18}
t_{i-4}	$\frac{1}{15}$	c_{18}

Окончательное решение примем за счет обобщения результатов, полученных на предыдущем этапе и по каждому классификатору a_1–a_n. Итоговый результат определим простым большинством результатов. Применим нечетные n, чтобы избежать случаи равного числа голосов для отличающихся классов c. Блок-схема алгоритма представлена на рис. 3.

Полученные результаты

Разработанный метод за счет комбинированного подхода позволил, не увеличивая числа отобранных согласно [8] признаков, существенно повысить показатели качества классификации и быстроту реагирования на инциденты ИБ и физические воздействия на КФС. На рис. 4 в сравнении показаны результаты применения предложенного подхода и стандартного метода, не учитывающего степень предпочтения результатов идентификации в различные дискретные моменты времени. При $N = 1$ решение задачи сводится к определению состояния КФС в дискретный момент времени. Применение разработанного подхода позволило повысить F-меру по сравнению со стандартным методом. Исходя из анализа гистограммы сделаем вывод, что оптимальное значение — величина отрезка идентификации $N = 4$. Отметим, что дальнейшее увеличение отрезка практически не приводит к увеличению F-меры. Решающий фактор для выбора величины скользящего окна N и количества классификаторов n — максимизация F-меры результатов классификации для контролируемой КФС.

Выполним сравнение результатов настоящего исследования с данными, полученными в научных работах [13–19]. Сравнение проведено на идентичном наборе исходных данных, выделены примененные другими исследователями методы (табл. 3).

На рис. 5, *а* представлена диаграмма точности (precision). Как видно, точность идентификации состо-

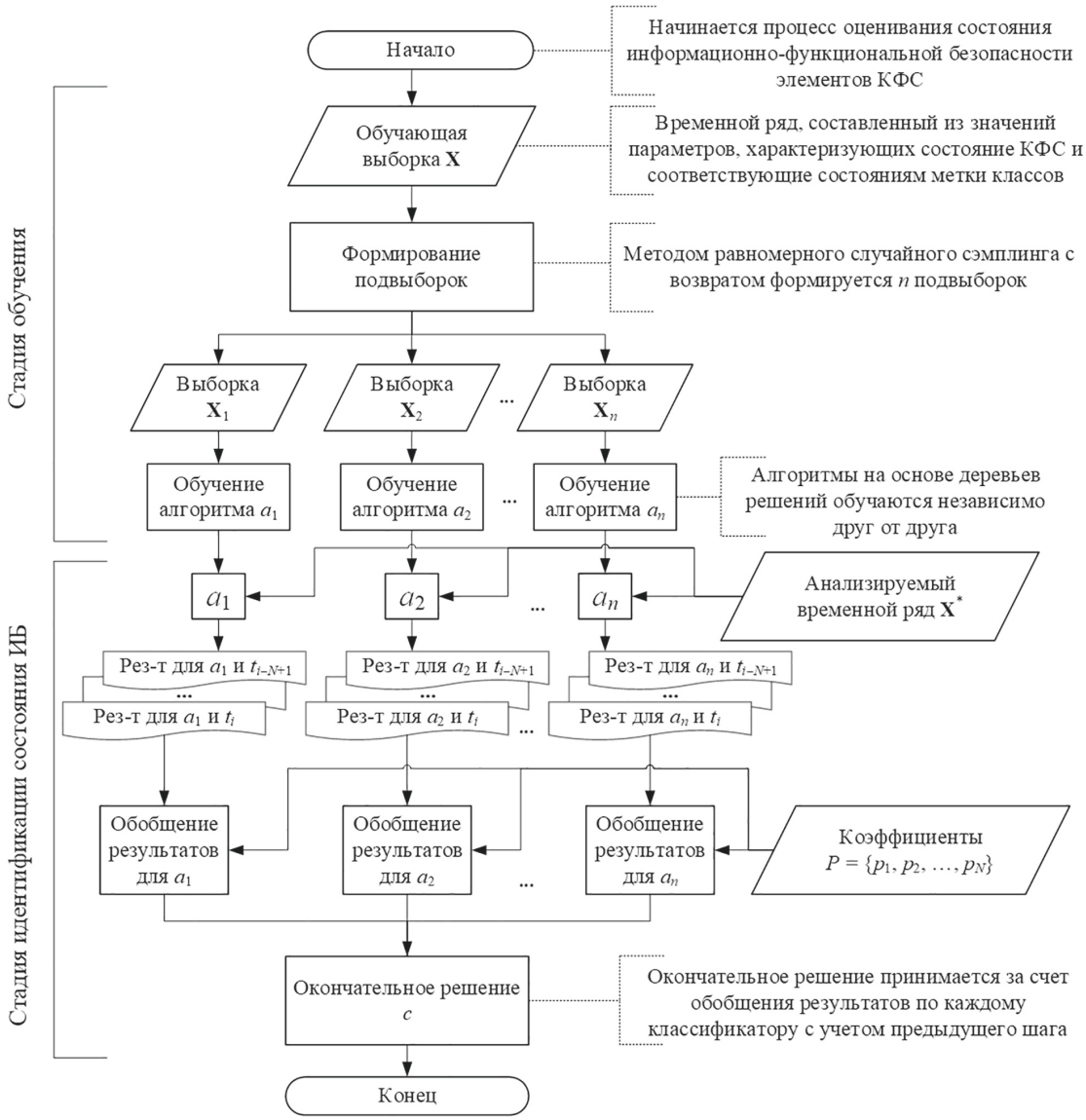

Рис. 3. Блок-схема алгоритма идентификации состояния киберфизических систем

Fig. 3. Block diagram of the algorithm for identifying the state of cyber-physical systems state

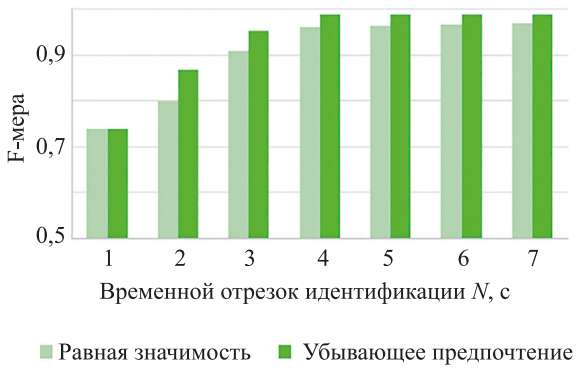

Рис. 4. F-мера при варьировании временного отрезка идентификации

Fig. 4. F-measure under varying the time interval of identification

яния элементов КФС с применением разработанного метода существенно выше, чем в работах других исследователей, применивших иные по природе классификаторы и методы предварительной обработки данных.

Разработанный метод позволил также повысить полноту (recall) идентификации состояния КФС (рис. 5, *b*). Методики с высокой полнотой классификации предпочтительнее для распознавания ранее неизвестных типов аномалий [20].

Таким образом, проанализированные работы других исследователей характеризуются относительно низкой полнотой идентификации состояний КФС, что является их существенным недостатком, поскольку такие модели могут идентифицировать значительное число атак на КФС как безопасные состояния.

Таблица 3. Исследования, с которыми произведено сравнение результатов
Table 3. Studies against which the results were compared

Авторы исследований	Применяемый метод	Обозначение	Источник
Kravchik M., Shabtai A.	Одномерные сверточные нейронные сети (One-Dimensional Convolutional Neural Networks)	1D СНС (1D CNN)	[13]
Shalyga D., Filonov P., Lavrentyev A.	Многослойный перцептрон (Multilayered Perceptron)	МП (MLP)	[14]
	Сверточные нейронные сети (Convolutional Neural Networks)	СНС (CNN)	
	Рекуррентные нейронные сети (Recurrent Neural Networks)	РНС (RNN)	
Inoue J., Yamagata Y., Chen Y., Poskitt C.M., Sun J.	Глубинные Нейронные Сети (Deep Neural Networks)	ГНС (DNN)	[15]
	Одноклассовый метод опорных векторов (One-Class Support Vector Machines)	МОВ (OCSVM)	
Kravchik M., Shabtai A.	Автоэнкодер (Autoencoder)	АК (AE)	[16]
Elnour M., Meskin N., Khan K., Jain R.	Изолирующие леса (Isolation Forests)	ИЛ (IF)	[17]
Li D., Chen D., Jin B., Shi L., Goh J., Ng S.K.	Генеративно-состязательные сети (Generative Adversarial Networks)	ГСНС (GAN)	[18]
Gomez A., Maimo L., Celdran A., Clemente F.	Нейронные сети с долгой краткосрочной памятью (Long Short-Term Memory Neural Networks)	LSTM ИНС (LSTM NN)	[19]

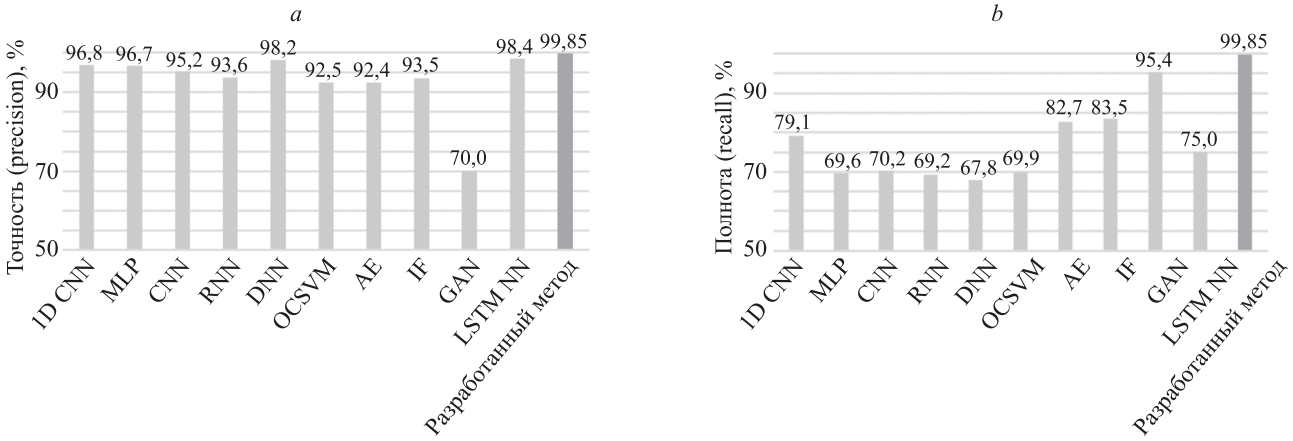

Рис. 5. Сравнение точности (*a*) и полноты (*b*) идентификации состояния киберфизических систем
Fig. 5. Comparison of precision (*a*) and recall (*b*) of identification of the cyber-physical systems state

Заключение

В работе представлен метод обработки данных мониторинга состояния информационно-функциональной безопасности киберфизических систем на основе анализа временных рядов с применением весовых коэффициентов значимости. Метод имеет важное значение для совершенствования средств обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной и функциональной безопасности, а также расследования инцидентов информационной безопасности в автоматизированных информационных системах.

Предложенный метод позволил существенно повысить скорость идентификации состояния элементов киберфизических систем за счет применения ансамбля параллельно работающих классификаторов. Ошибки из-за случайных отклонений параметров функционирования киберфизических систем сокращаются с помощью обобщения и взвешенного усреднения результатов идентификации на временном отрезке. Точность идентификации, по сравнению с лучшими подходами, представленными в научных работах, при использовании разработанного метода увеличилась на 1,45 %, полнота — на 4,45 % и составила 99,85 % для обоих показателей. Снижение вычислительных затрат и увеличение скорости идентификации состояния элементов киберфизических систем — решающие факторы при осуществлении мониторинга и восстановлении безопасного функционирования.

Разработанный метод является новой альтернативой и дополнением к существующим программным и программно-аппаратным средствам. В качестве дальнейших перспектив исследования можно отметить разработку методов и методик противодействия выявленным нарушениям на основе принципа обратной связи в режиме реального времени.

Литература

1. Shukalov A.V., Zakoldaev D.A., Zharinov I.O., Zharinov O.O. Control, computing and communication in industrial cyberphysical systems with feedback // Journal of Physics: Conference Series. 2021. V. 2094. N 4. P. 042036. https://doi.org/10.1088/1742-6596/2094/4/042036
2. Котенко И.В., Крибель А.М., Лаута О.С., Саенко И.Б. Анализ процесса самоподобия сетевого трафика как подход к обнаружению кибератак на компьютерные сети // Электросвязь. 2020. № 12. С. 54–59. https://doi.org/10.34832/ELSV.2020.13.12.008
3. Васильев В.И., Вульфин А.М., Гвоздев В.Е., Картак В.М., Атарская Е.А. Обеспечение информационной безопасности киберфизических объектов на основе прогнозирования и обнаружения аномалий их состояния // Системы управления, связи и безопасности. 2021. № 6. С. 90–119. https://doi.org/10.24412/2410-9916-2021-6-90-119
4. Зегжда Д.П., Павленко Е.Ю. Гомеостатическая стратегия безопасности киберфизических систем // Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 9–23.
5. Зайцева Е.А., Зегжда Д.П., Полтавцева М.А. Использование графового представления и прецедентного анализа для оценки защищенности компьютерных систем // Проблемы информационной безопасности. Компьютерные системы. 2019. № 2. С. 136–148.
6. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. 2016. V. 50. N 8. P. 673–681. https://doi.org/10.3103/S0146411616080125
7. Васильев Ю.С., Зегжда П.Д., Зегжда Д.П. Обеспечение безопасности автоматизированных систем управления технологическими процессами на объектах гидроэнергетики // Известия Российской академии наук. Энергетика. 2016. № 3. С. 49–61.
8. Семенов В.В. Подход к формированию информативных признаков в задачах мониторинга информационной безопасности киберфизических систем // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. № 6. С. 887–894. https://doi.org/10.17586/2226-1494-2021-21-6-887-894
9. Семенов В.В. Оценивание состояния информационной безопасности на основе анализа временных рядов // Научно-технический вестник Поволжья. 2021. № 10. С. 127–129.
10. Kruegel C., Toth T. Using decision trees to improve signature-based intrusion detection // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2003. V. 2820. P. 173–191. https://doi.org/10.1007/978-3-540-45248-5_10
11. Cagli E., Dumas C., Prouff E. Convolutional neural networks with data augmentation against jitter-based countermeasures // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2017. V. 10529. P. 45–68. https://doi.org/10.1007/978-3-319-66787-4_3
12. Goh J., Adepu S., Junejo K.N., Mathur A. A dataset to support research in the design of secure water treatment systems // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2017. V. 10242. P. 88–99. https://doi.org/10.1007/978-3-319-71368-7_8
13. Kravchik M., Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks // Proc. of the 47th Workshop on Cyber-Physical Systems Security and PrivaCy. 2018. P. 72–83. https://doi.org/10.1145/3264888.3264896
14. Shalyga D., Filonov P., Lavrentyev A. Anomaly detection for water treatment system based on neural network with automatic architecture optimization // arXiv. 2018. arXiv:1807.07282. https://doi.org/10.48550/arXiv.1807.07282
15. Inoue J., Yamagata Y., Chen Y., Poskitt C.M., Sun J. Anomaly detection for a water treatment system using unsupervised machine learning // Proc. of the 17th IEEE International Conference on Data Mining Workshops (ICDMW). 2017. P. 1058–1065. https://doi.org/10.1109/ICDMW.2017.149

References

1. Shukalov A.V., Zakoldaev D.A., Zharinov I.O., Zharinov O.O. Control, computing and communication in industrial cyberphysical systems with feedback. *Journal of Physics: Conference Series*, 2021, vol. 2094, no. 4, pp. 042036. https://doi.org/10.1088/1742-6596/2094/4/042036
2. Kotenko I.V., Kribel A.M., Lauta O.S., Saenko I.B. Analysis of the process of selfsimilarity of network traffic as an approach to detecting cyber attacks on computer networks. *Electrosvyaz Magazine*, 2020, no. 12, pp. 54–59. (in Russian). https://doi.org/10.34832/ELSV.2020.13.12.008
3. Vasilyev V.I., Vulfin A.M., Gvozdev V.E., Kartak V.M. Atarskaya E.A. Ensuring information security of cyber-physical objects based on predicting and detecting anomalies in their state. *Systems of Control, Communication and Security*, 2021, no. 6, pp. 90–119. (in Russian). https://doi.org/10.24412/2410-9916-2021-6-90-119
4. 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)
5. Zaitceva E.A., Zegzhda D.P., Poltavtseva M.A. Applying of graph representation and case-based reasoning for security evaluation of computer systems. *Information Security Problems. Computer Systems*, 2019, no. 2, pp. 136–148. (in Russian)
6. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things. *Automatic Control and Computer Sciences*, 2016, vol. 50, no. 8, pp. 673–681. https://doi.org/10.3103/S0146411616080125
7. Vasiliev Y.S., Zegzhda P.D., Zegzhda D.P. Providing security for automated process control systems at hydropower engineering facilities. *Thermal Engineering*, 2016, vol. 63, no. 13, pp. 948–956. https://doi.org/10.1134/S0040601516130073
8. Semenov V.V. An approach to the identification of the state of elements in cyber-physical systems based on principal component analysis. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 6, pp. 887–894. (in Russian). https://doi.org/10.17586/2226-1494-2021-21-6-887-894
9. Semenov V.V. Assessment of information security state based on analysis of time series. *Scientific and Technical Volga region Bulletin*, 2021, no. 10, pp. 127–129. (in Russian)
10. Kruegel C., Toth T. Using decision trees to improve signature-based intrusion detection. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2003, vol. 2820, pp. 173–191. https://doi.org/10.1007/978-3-540-45248-5_10
11. Cagli E., Dumas C., Prouff E. Convolutional neural networks with data augmentation against jitter-based countermeasures. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10529, pp. 45–68. https://doi.org/10.1007/978-3-319-66787-4_3
12. Goh J., Adepu S., Junejo K.N., Mathur A. A dataset to support research in the design of secure water treatment systems. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10242, pp. 88–99. https://doi.org/10.1007/978-3-319-71368-7_8
13. Kravchik M., Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks. *Proc. of the 47th Workshop on Cyber-Physical Systems Security and PrivaCy*, 2018, pp. 72–83. https://doi.org/10.1145/3264888.3264896
14. Shalyga D., Filonov P., Lavrentyev A. Anomaly detection for water treatment system based on neural network with automatic architecture optimization. *arXiv*, 2018, arXiv:1807.07282. https://doi.org/10.48550/arXiv.1807.07282
15. Inoue J., Yamagata Y., Chen Y., Poskitt C.M., Sun J. Anomaly detection for a water treatment system using unsupervised machine learning. *Proc. of the 17th IEEE International Conference on Data*

16. Kravchik M., Shabtai A. Efficient cyber attack detection in industrial control systems using lightweight neural networks and PCA // IEEE Transactions on Dependable and Secure Computing. 2022. V. 19. N 4. P. 2179–2197. https://doi.org/10.1109/TDSC.2021.3050101
17. Elnour M., Meskin N., Khan K., Jain R. A dual-isolation-forests-based attack detection framework for industrial control systems // IEEE Access. 2020. V. 8. P. 36639–36651. https://doi.org/10.1109/ACCESS.2020.2975066
18. Li D., Chen D., Jin B., Shi L., Goh J., Ng S.-K. MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2019. V. 11730. P. 703–716. https://doi.org/10.1007/978-3-030-30490-4_56
19. Gómez A., Maimó L., Celdrán A., Clemente F. MADICS: A methodology for anomaly detection in industrial control systems // Symmetry. 2020. V. 12. N 10. P. 1583. https://doi.org/10.3390/sym12101583
20. Гайфулина Д.А., Котенко И.В. Анализ моделей глубокого обучения для задач обнаружения сетевых аномалий Интернета вещей // Информационно-управляющие системы. 2021. № 1. С. 28–37. https://doi.org/10.31799/1684-8853-2021-1-28-37

Mining Workshops (ICDMW), 2017, pp. 1058–1065. https://doi.org/10.1109/ICDMW.2017.149
16. Kravchik M., Shabtai A. Efficient cyber attack detection in industrial control systems using lightweight neural networks and PCA. *IEEE Transactions on Dependable and Secure Computing*, 2022, vol. 19, no. 4, pp. 2179–2197. https://doi.org/10.1109/TDSC.2021.3050101
17. Elnour M., Meskin N., Khan K., Jain R. A dual-isolation-forests-based attack detection framework for industrial control systems. *IEEE Access*, 2020, vol. 8, pp. 36639–36651. https://doi.org/10.1109/ACCESS.2020.2975066
18. Li D., Chen D., Jin B., Shi L., Goh J., Ng S.-K. MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11730, pp. 703–716. https://doi.org/10.1007/978-3-030-30490-4_56
19. Gómez A., Maimó L., Celdrán A., Clemente F. MADICS: A methodology for anomaly detection in industrial control systems. *Symmetry*, 2020, vol. 12, no. 10, pp. 1583. https://doi.org/10.3390/sym12101583
20. Gaifulina D.A., Kotenko I.V. Analysis of deep learning models for network anomaly detection in Internet of Things. *Informatsionno-Upravliaiushchie Sistemy*, 2021, no. 1, pp. 28–37. (in Russian). https://doi.org/10.31799/1684-8853-2021-1-28-37

Автор

Семенов Виктор Викторович — кандидат технических наук, младший научный сотрудник, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, 199178, Российская Федерация, SC 57204123255, https://orcid.org/0000-0002-7216-769X, v.semenov@spcras.ru

Author

Viktor V. Semenov — PhD, Junior Researcher, St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg, 199178, Russian Federation, SC 57204123255, https://orcid.org/0000-0002-7216-769X, v.semenov@spcras.ru

Статья поступила в редакцию 20.06.2022
Одобрена после рецензирования 03.10.2022
Принята к печати 22.11.2022

Received 20.06.2022
Approved after reviewing 03.10.2022
Accepted 22.11.2022