УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2021 Том 21 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2021 Vol. 21 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

COMPUTER SCIENCE

doi: 10.17586/2226-1494-2021-21-6-887-894
УДК 004.021

Подход к формированию информативных признаков в задачах мониторинга информационной безопасности киберфизических систем

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. Тесная интеграция современных киберфизических систем с системами производственно-технологическими и критической информационной инфраструктуры требует совершенствования процесса мониторинга. Процесс мониторинга необходим при постоянном увеличении возможных точек вхождения в системы. Для обработки большого количества данных, поступающих от систем мониторинга, необходимы значительные вычислительные мощности. В этой связи актуальным является снижение размерности признакового пространства при сохранении приемлемой точности мониторинга. Предлагаемое решение должно быть инвариантно к размерности и порядкам величин, из которых составлены временные ряды, подаваемые на вход системы. **Метод.** Для выделения наиболее информативных признаков при формировании их набора предложено применять метод анализа главных компонент, а для их классификации — метод на основе деревьев решений. **Основные результаты.** Выполнен вычислительный эксперимент для подтверждения применимости разработанного подхода. В эксперименте использовались данные сетевого трафика исследовательского стенда киберфизической системы водоочистки. Точность совокупности методов на анализируемых данных составила 98,74 %. Результаты сравнения с известными исследованиями показали увеличение F-меры до 0,925, что на 4,8 % превышает наиболее результативный из применяемых на сегодняшний день методов — метод изолирующего леса (Isolation Forest). **Практическая значимость.** Разработанный подход позволяет существенно повысить скорость идентификации и с высокой точностью обнаруживать аномалии информационной и функциональной безопасности киберфизических систем за счет снижения размерности исходного признакового пространства. Предложенный подход может использоваться в системах мониторинга событий информационной безопасности. Представленные теоретические результаты могут быть полезны исследователям информационно-функциональной безопасности киберфизических систем.

Ключевые слова

информационная безопасность, функциональная безопасность, киберфизические системы, выявление аномалий, анализ временных рядов, метод главных компонент, системы мониторинга

Ссылка для цитирования: 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. doi: 10.17586/2226-1494-2021-21-6-887-894

An approach to the identification of the state of elements in cyber-physical systems based on principal component 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 close integration of modern cyber-physical systems with production and technological ones as well as with critical information infrastructure requires improving the monitoring process. The monitoring process is necessary with

a constant increase in the possible points of entry into the system. The processing of a large amount of data coming from monitoring systems requires significant computing power. In this regard, it is relevant to reduce the dimension of the feature space while maintaining an acceptable monitoring accuracy. The proposed solution should be invariant to the dimension and orders of magnitude from which the time series supplied to the input of the monitoring system are composed. To obtain the most informative features in the formation of their set, it is proposed to use principal component analysis, and a method based on decision trees for their classification. A computational experiment was performed to confirm the applicability of the developed approach. The data of the network traffic for the research stand of the cyber-physical system water treatment were used in the experiment. The accuracy of the set of methods on the analyzed data was 98.74 %. The comparison with known studies showed an increase in the F-measure up to 0.925, which is 4.8 % higher than the most effective method used to date, namely the Isolation Forest method. The developed approach allows one to significantly increase the speed of identification and to detect anomalies of information security and functional safety of cyber-physical systems with high accuracy by reducing the dimension of the original feature space. The proposed approach can be used in event monitoring systems that deal with information security. The presented theoretical results can be useful for researchers of information security and functional safety of cyber-physical systems.

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

For citation: 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). doi: 10.17586/2226-1494-2021-21-6-887-894

Введение

Быстрое развитие технологий «Индустрии 4.0» привело к включению киберфизических систем в приоритетный список инноваций, являющихся критически важными для защиты национальных интересов Российской Федерации. Киберфизическая система (КФС) — система, подразумевающая интеграцию вычислительных ресурсов в физические сущности любого вида [1]. КФС, являясь основой для реализаций множества современных инновационных решений, существенно уязвимы с точки зрения успешных информационных атак, приводящих к критическим сбоям или аномальному функционированию [2].

Ввиду тесной интеграции КФС в производственно-технологические системы, системы критической информационной инфраструктуры, а также значительного количества возможных точек вхождения, задача мониторинга информационной безопасности (ИБ) для КФС является более сложной, чем для классических информационных систем [3]. В случае реализации угроз ИБ основной целью злоумышленника, как правило, является получение возможности управления КФС при помощи информационных воздействий [4], при этом деструктивные информационные воздействия могут влиять как на процессы хранения, обработки и передачи информации внутри системы, так и на физические процессы исполнительных механизмов КФС.

На сегодняшний день имеется множество работ отечественных и зарубежных исследователей, посвященных разработке методов, методик и систем обнаружения нарушений ИБ КФС [5–7]. Существенная часть исследователей рассматривает вопросы выявления аномалий ИБ КФС [8], которые могут быть вызваны атаками злоумышленников, например, внедрением программных закладок в КФС [9].

В случае крупномасштабных КФС, в которых присутствует огромное множество датчиков и логов протекающих информационных процессов, снижение размерности признакового пространства приобретает особую актуальность из-за огромного количества данных, поступающих от систем мониторинга, требующих несоизмеримо высоких вычислительных мощностей для их обработки.

В связи с этим особую актуальность приобретают методы и алгоритмы, позволяющие с минимальными затратами времени и вычислительных ресурсов производить мониторинг состояния информационной и функциональной безопасности КФС с приемлемой для практического использования точностью.

Постановка задачи

КФС реализует заранее определенные ее техническими особенностями функции и представляет собой замкнутую систему, в которой протекает конечное множество физических процессов [10]. Предположим, что существует множество объектов обучающей выборки $\{o_1, \ldots, o_m\} = \{\{x_1(t_1), x_2(t_1), \ldots, x_s(t_1)\}, \ldots, \{x_1(t_m), x_2(t_m), \ldots, x_n(t_m)\}\} \subset X$, составленных из временных рядов, характеризующих функционирование КФС или ее отдельных элементов, множество меток классов $\{C_0, C_1\} \subset C$, отражающих состояния ИБ. Требуется построить алгоритм μ, способный соотнести элементы множества X с одним из известных классов, соотнесенных с состоянием ИБ:

$$\mu: X \to C,$$

где C_0 и C_1 — множество меток классов безопасных состояний ИБ КФС и аномальных (опасных) состояний ИБ; $\{c_1, c_2, \ldots, c_k\} \subset C_0$, $\{c_{k+1}, c_{k+2}, \ldots, c_l\} \subset C_1$, l — число идентифицируемых состояний ИБ КФС; m — число объектов в обучающей выборке.

Цель работы — разработка научного подхода, обеспечивающего увеличение скорости идентификации состояния ИБ в условиях их большого количества и ограниченности обучающей выборки.

Предлагаемый подход

Универсальным способом представления динамически изменяющихся данных являются временные

ряды [11]. Временной ряд X — собранный в разные моменты времени статистический материал о значении каких-либо параметров исследуемого процесса КФС. $X = \{x(t_1), x(t_2), \ldots, x(t_m)\}$ — полученные значения, которые являются следствием протекания процессов КФС. Оценивание защищенности КФС от информационных угроз на основе анализа временных рядов сведем к задаче классификации их элементов и выявлению значений, относящихся к небезопасному классу C_1 [12]. Обилие в КФС циклических (повторяющихся) процессов определяет успешную применимость предлагаемого подхода. В исследуемой задаче формируется m элементов временных рядов $X = \{\{x_1(t_1), x_2(t_1), \ldots, x_n(t_1)\}, \{x_1(t_2), x_2(t_2), \ldots, x_n(t_2)\}, \ldots, \{x_1(t_m), x_2(t_m), \ldots, x_n(t_m)\}\}$, представляющих собой сгруппированные и синхронизированные по времени множества значений сигналов от n источников.

Таким образом, получим метку класса состояния ИБ КФС в дискретный момент времени t:

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

где t — метка времени, $t = 1, \ldots, m$; D_f — множество допустимых значений признака; s — количество отобранных наиболее информативных признаков.

Исходное признаковое пространство $H = (f_1, f_2, \ldots, f_n)$ представляет собой набор возможных параметров функционирования КФС, которые могут включать в себя как характеристики информационных процессов (например, параметры сетевого трафика), так и данные о протекающих физических процессах (например, информацию с датчиков). Очевидно, что крайне важным является выявление признаков, способствующих достижению максимальной полноты и точности идентификации.

Наилучший подход для оценивания информативности признаков в задаче идентификации состояния ИБ КФС — информационный подход. Данный подход позволяет выполнить отбор признаков, обладающих максимальной дискриминаторной способностью для защищаемого типа КФС.

Метод анализа главных компонент (МГК) широко используется для понижения размерности исходных данных. В работах [13, 14] МГК применяется в качестве предобработки, при этом исходное многомерное признаковое пространство преобразуется в пространство главных компонент (ГК). В настоящей работе МГК предложено использовать с целью вычисления информативности каждого признака (источника информации о процессах системы).

Матрица данных $\mathbf{X}$ представляет собой результаты измерения некоторых параметров объекта КФС во времени:

$$\mathbf{X} = \begin{pmatrix} x_1(t_1) & x_2(t_1) & \ldots & x_n(t_1) \\ x_1(t_2) & x_2(t_2) & \ldots & x_n(t_2) \\ \ldots & \ldots & \ldots & \ldots \\ x_1(t_m) & x_2(t_m) & \ldots & x_n(t_m) \end{pmatrix}.$$

Перед применением МГК для анализа обучающей выборки КФС, выполним автошкалирование (центрирование и нормировку) данных. Каждая строка матрицы $\mathbf{X}$ — матрицы временных рядов предобработанных данных, состоит из параметров, описывающих состояние ИБ КФС.

Разложение матрицы $\mathbf{X}$ в виде матричного уравнения при помощи метода анализа ГК представлено в виде:

$$\mathbf{X} = \mathbf{T}\mathbf{P}^T + \mathbf{E},$$

где $\mathbf{T}$ — матрица счетов (*scores*); $\mathbf{P}^T$ — транспонированная матрица нагрузок (*loadings*); $\mathbf{E}$ — матрица остатков (*errors or residuals*); индекс «^{T}» — операция транспонирования, в результате которой матрица поворачивается относительно своей главной диагонали.

Каждый столбец $\mathbf{P}$ — вектор ГК, число строк — n (размерность пространства данных), число столбцов — k (количество векторов ГК, выбранных для проецирования). Величины нагрузок p — принадлежат диапазону [–1, +1] и отражают влияние на данную ГК конкретной исходной переменной.

Матрица ошибок (или остатков): $\mathbf{E} = \mathbf{X} - \mathbf{T}\mathbf{P}^T$.

Для вычисления информативности признаков необходимо решить задачу выбора числа ГК (k). Для этого последовательно при каждом значении k, начиная с единицы, рассчитаем значения объясненной дисперсии (ERV):

$$ERV = 1 - \sum_{t=1}^{m}\sum_{j=1}^{n} e^2_{t,j} \Big/ \sum_{t=1}^{m}\sum_{j=1}^{n} x^2_{t,j},$$

где $e_{t,j}$ и $x_{t,j}$ — элементы матриц $\mathbf{E}_t$ и $\mathbf{X}_t$ соответственно.

Решающее правило для выбора k: $ERV_k \geqslant \varepsilon$, где ε выбирается эмпирически в зависимости от конкретной КФС. Тогда, информативность i-го признака при k ГК вычисляется при помощи матрицы $\mathbf{P}$ по формуле:

$$I_{fi} = \sqrt{\sum_{j=1}^{k} p^2_{t,j}}. \qquad (1)$$

Идентификаторы источников упорядочиваются по информативности $I_{f1} \geqslant I_{f2} \geqslant \ldots \geqslant I_{fs}$. По правилу Кайзера произведем отбор s источников, информативность которых больше средней информативности:

$$I_{fi} > \frac{1}{n}\sum_{i=1}^{n} I_{fi},$$

где $\frac{1}{n}\sum_{i=1}^{n} I_{fi}$ — средняя информативность всех рассматриваемых (доступных) источников; $i = 1, \ldots, n$.

Идентификаторы источников заносятся в архив и участвуют в дальнейшем построении модели классификации. Блок-схема алгоритма представлена на рис. 1.

Эксперимент

С целью исследования состояния ИБ выполним анализ сетевого трафика между системой управления и сбора данных (SCADA) и программируемым логическим контроллером КФС. Апробация метода заключается в проведении вычислительного эксперимента над набором данных [15] с целью практической реализации предложенного подхода.

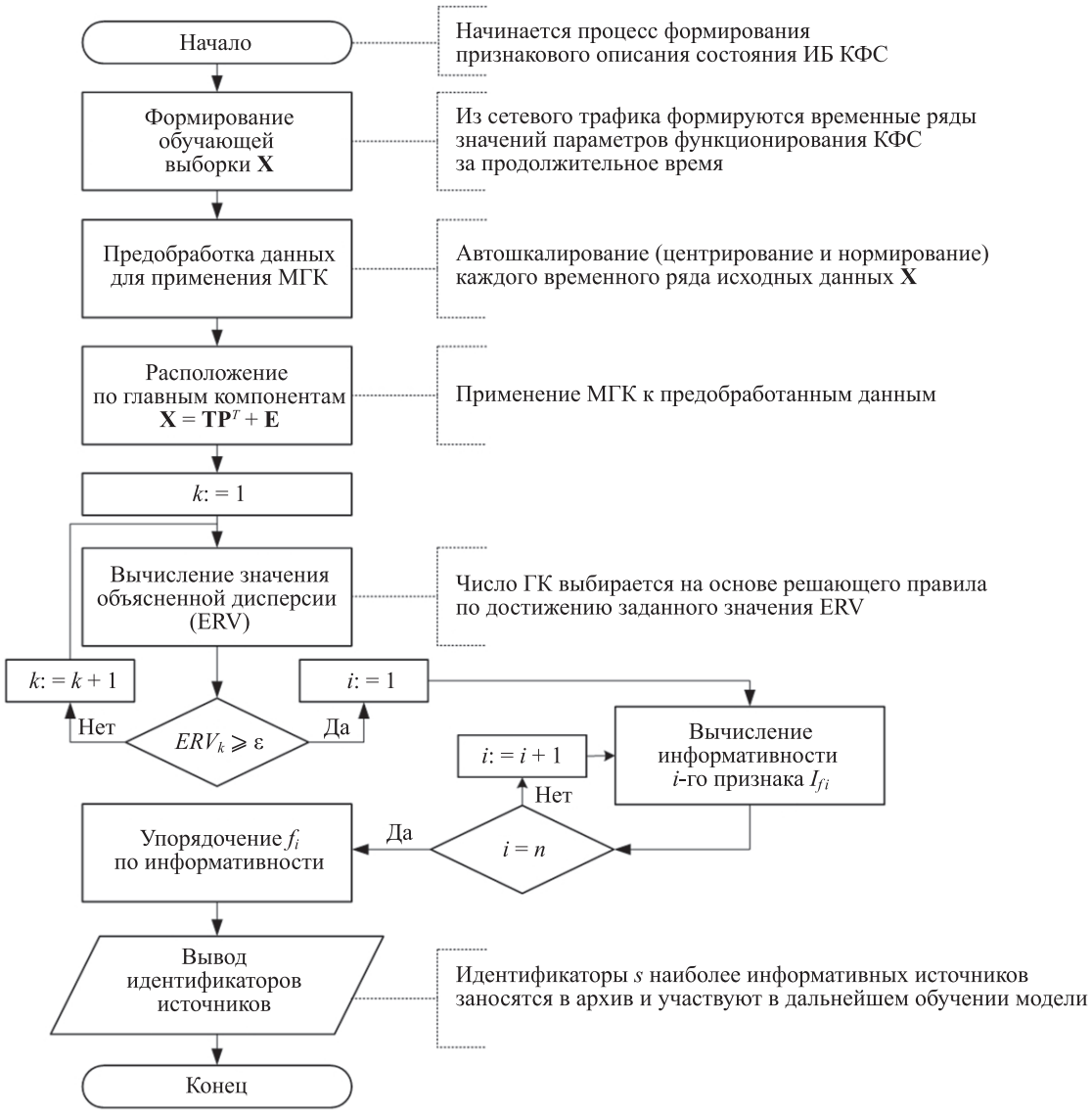

Рис. 1. Блок-схема алгоритма формирования признакового описания состояния информационной безопасности элементов киберфизических систем

Fig. 1. Block diagram of the algorithm for the formation of feature description of the information security state of cyber-physical systems elements

Цель вычислительного эксперимента — применение алгоритма формирования признакового описания состояния ИБ элементов КФС для реально существующей КФС.

Для анализа временных рядов, характеризующих функционирование КФС, применено программное обеспечение Matlab R2021a. Исходные данные для реализации разработанного комплексного подхода представляют численный двумерный массив 944 919 × 51, каждый элемент массива **X** задан двумя индексами, индексом строки и индексом столбца. В строках расположены значения временных рядов, регистрируемых раз в секунду, в свою очередь столбцы упорядочены по источникам получения информации от КФС.

Перечень источников получения информации о функционировании КФС представлен в работе [15]: FIT101, LIT101, MV101, P101, P102, AIT201, AIT202, AIT203, FIT201, MV201, P201, P202, P203, P204, P205, P206, DPIT301, FIT301, LIT301, MV301, MV302, MV303, MV304, P301, P302, AIT401, AIT402, FIT401, LIT401, P401, P402, P403, P404, UV401, AIT501, AIT502, AIT503, AIT504, FIT501, FIT502, FIT503, FIT504, P501, P502, PIT501, PIT502, PIT503, FIT601, P601, P602, P603.

На первом этапе реализации алгоритма формирования информативных признаков выполним разложение при помощи стандартной функции Matlab [*loadings*, *scores*, *latent*, *tsquared*, *explained*, *mu*] = pca(X, *'NumComponents'*, 51), где:

— *loadings* — матрица нагрузок;
— *scores* — матрица счетов;
— *latent* — вектор-столбец, содержащий значения дисперсий ГК, т. е. собственные значения ковариационной матрицы **X**;
— *tsquared* — вектор-столбец, который представляет собой сумму квадратов стандартизованных счетов

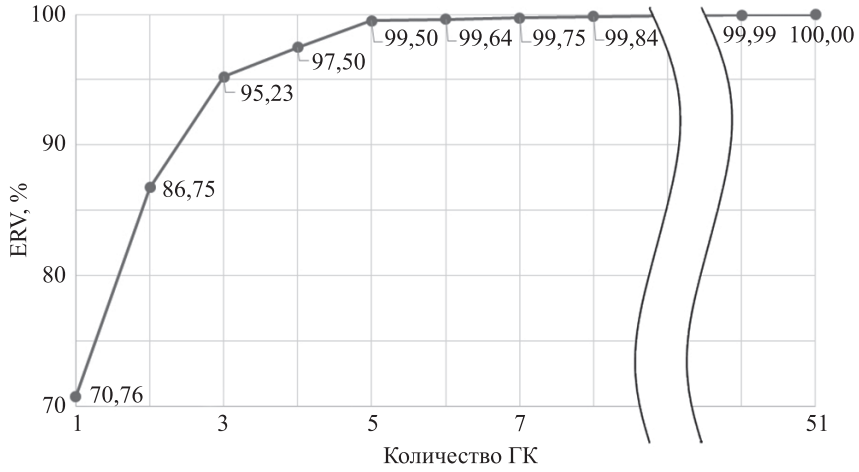

Рис. 2. Зависимость совокупной объясненной дисперсии от количества главных компонент для исследуемой киберфизической системы водоочистки

Fig. 2. Dependence of the explained residual variance on the amount of principal components for the studied water treatment cyber-physical system

для каждого временного ряда (Т-квадрат распределения Хотеллинга);

— *explained* — вектор-столбец, содержащий значения объясненной дисперсии для заданного в *NumComponents* числа ГК;

— *mu* — средние значения переменных в **X**, возвращенные как вектор-строка.

Наиболее интересными для анализа и формирования информативных признаков являются переменные *loadings* и *explained*. Последняя представляет собой столбец, в котором содержатся частные значения дисперсии по каждой ГК отдельно. Для получения совокупных значений в цикле производится суммирование q первых элементов:

$$ERV_q = \sum_{i=1}^{q} explained(i),\ q = 1, \ldots, n.$$

Зависимость совокупной объясненной дисперсии от количества ГК представлена на рис. 2.

ГК упорядочиваются по величинам ERV. Как видно из графика (рис. 2), значения объясненной дисперсии резко увеличиваются при ГК с первой по пятую, затем идет монотонное медленное увеличение вплоть до 51-ой ГК. Исходя из этого, можно сделать вывод, что бóльшую часть разброса экспериментальных данных можно объяснить существенно меньшим числом источников в пространстве ГК. Разработанная модель подразумевает использование МГК для вычисления информативности признаков с целью сокращения вычислительных затрат.

Для непосредственного расчета информативности используется массив *loadings*, строки которого упорядочены по источникам f_i, а столбцы содержат значения нагрузок **P** для каждой из k ГК. Старшинство ГК определяется бóльшим значением величины объясненной дисперсии. На рис. 3 представлен график нагрузок для двух старших ГК, по оси абсцисс отложены значения 1-го столбца матрицы нагрузок **P** ($p_{i,1}$), а по оси ординат — второго **P** ($p_{i,2}$). По мере удаления от начала координат и увеличения абсолютных значений координат точки информативность соответствующего источника увеличивается. Отметим, что при разном количестве ГК (k) результаты расчета информативности отличаются несущественно, главное влияние оказывают пять старших ГК.

Информативность признаков по разработанному алгоритму рассчитана по формуле (1).

В результате расчетов в соответствии с информативностью i-го признака (f_i) при k ГК определены наиболее информативные (по правилу Кайзера) признаки для: LIT401 информативность (I_{fi}) равна 0,99913; LIT101 — 0,99913; LIT301 — 0,99896; AIT201 — 0,94786; PIT501 — 0,67211; PIT503 — 0,51464; AIT402 — 0,48828; AIT203 — 0,31012; AIT502 — 0,22888, а также информативные признаки, например: DPIT301 — 0,04848; AIT504 — 0,02570; AIT503 — 0,01251; FIT201 — 0,00883, которые имеют значения менее 0,1.

Из 51 ГК источника информации о функционировании КФС информативность девяти оказалась больше средней информативности, составившей $\bar{I} = 0{,}12410$.

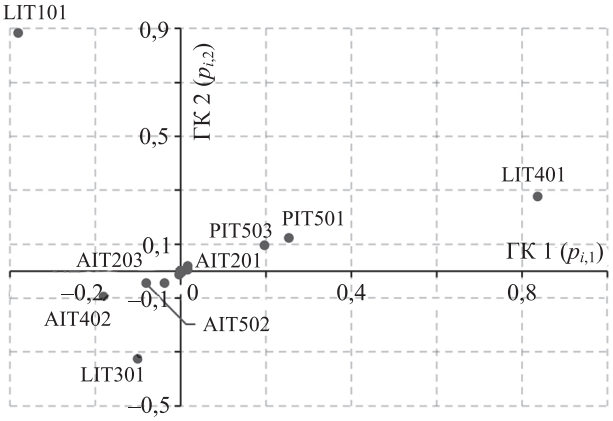

Рис. 3. График нагрузок при осуществлении атак на киберфизическую систему

Fig. 3. Schedule of loadings during the attacks on the cyber-physical system

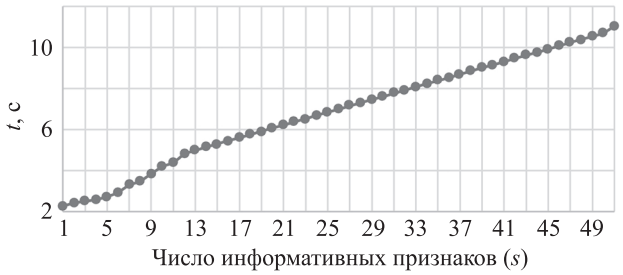

Рис. 4. Зависимость времени обучения классификатора от числа информативных признаков

Fig. 4. Dependence of the training time of the classifier on the number of informative features

Данный результат позволил существенно сократить количество используемых для построения модели классификации признаков, уменьшив тем самым вычислительные затраты на обработку массива данных и увеличив скорость реагирования на инциденты ИБ. Эксперимент показал закономерное увеличение времени обучения классификатора на основе деревьев решений при увеличении числа информативных признаков (рис. 4).

Модель формирования признакового описания состояния ИБ элементов КФС была применена для временных рядов, полученных в результате функционирования КФС водоочистки в безопасном и в потенциально опасных состояниях ИБ. Исследованы зависимости характеристик классификации от числа информативных признаков (рис. 5). При проведении эксперимента и построении графика в первую очередь использованы признаки с большей информативностью, вычисленной по формуле (1).

На графике (рис. 5) наблюдается резкое увеличение показателей качества идентификации при числе информативных признаков от одного до трех. Дальнейшее увеличение s также приводит к закономерному росту величины площади под ROC-кривой (AUC) и F-меры, тенденция сохраняется вплоть до девяти информативных признаков, после чего показатели меняются незначительно. При s = 9: точность 98,74 %, AUC — 0,96, F-мера — 0,925. При s = 51 AUC увеличилась всего на 0,01, а F-мера на 0,02 по сравнению с s = 9, что позволяет говорить о том, что большая часть источников содержит шумовые данные и не способствует существенному увеличению качества классификации. Эксперимент показал, что характеристики классификации зависят не только от числа информативных признаков, но и от порядка их использования — предпочтительнее обучать классификатор на значениях наиболее информативных признаков. Результаты исследования сопоставлены с работами [6, 13, 16–20]. Наилучшее из представленных в литературе решений основывается на применении метода изолирующего леса (Isolation Forest) [20], F-мера 0,882. Исходя из этого, можно сделать вывод о возможности комплексного применения предложенного подхода в целях существенного повышения оперативности мониторинга и сокращения вычислительных затрат.

Заключение

Предложенный подход к формированию признакового описания состояния информационной безопасности позволяет на этапах реализации мониторинга элементов киберфизических систем повысить полноту, точность и скорость мульти-классификации. Алгоритм инвариантен к размерности и порядкам величин, из которых составлены временные ряды, подаваемые на вход.

Полученные результаты демонстрируют применимость разработанного подхода, позволяющего повысить скорость идентификации состояний КФС и обеспечивающего эффективное уменьшение признакового пространства без существенной потери точности. Достигается значение F-меры 0,925, что на 4,8 % превышает наиболее результативный из представленных на сегодняшний день в мировой научной литературе метод на основе изолирующего леса.

В результате применения разработанного алгоритма возможно выделить наиболее информативные признаки, используемые в дальнейшем в системах управления информационной безопасностью и управления событиями безопасности.

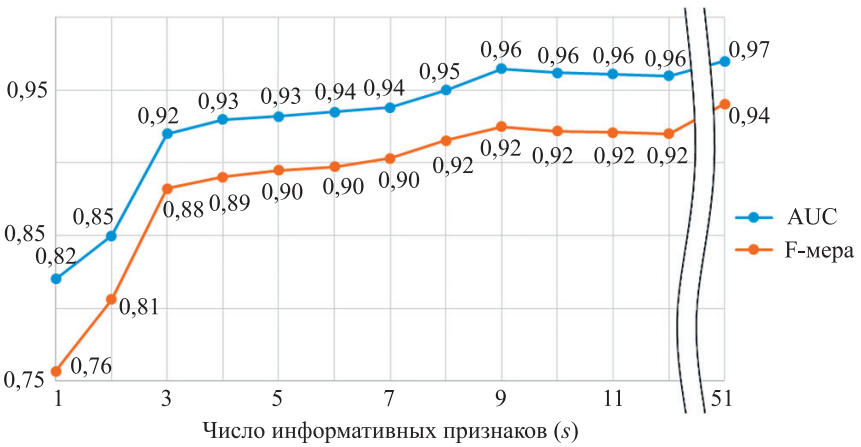

Рис. 5. Оценка качества классификации

Fig. 5. Assessment of the classification quality

Литература

1. Cardenas A., Amin S., Sinopoli B., Giani A., Perrig A., Sastry S. Challenges for securing cyber physical systems // Workshop on Future Directions in Cyber-Physical Systems Security. 2009.
2. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. № 2(26). С. 2–15. https://doi.org/10.21681/2311-3456-2018-2-2-15
3. Семенов В.В., Салахутдинова К.И., Лебедев И.С., Сухопаров М.Е. Выявление аномальных отклонений при функционировании устройств киберфизических систем // Прикладная информатика. 2019. Т. 14. № 6(84). С. 114–122. https://doi.org/10.24411/1993-8314-2019-10053
4. Zegzhda D.P. Sustainability as a criterion for information security in cyber-physical systems // Automatic Control and Computer Sciences. 2016. V. 50. № 8. C. 813–819. https://doi.org/10.3103/S0146411616080253
5. Павленко Е.Ю., Штыркина А.А., Зегжда Д.П. Оценка устойчивости киберфизических систем на основе спектральной теории графов // Проблемы информационной безопасности. Компьютерные системы. 2019. № 1. С. 60–68.
6. 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
7. Wang X., Zhou Q., Harer J., Brown G., Qiu S., Dou Z., Wang J., Hinton A., Gonzalez C.A., Chin P. Deep learning-based classification and anomaly detection of side-channel signals // Proceedings of SPIE. 2018. V. 10630. P. 1063006. https://doi.org/10.1117/12.2311329
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 // Lecture Notes in Computer Science. 2019. V. 11660. P. 104–112. https://doi.org/10.1007/978-3-030-30859-9_9
9. Meleshko A.V., Desnitsky V.A., Kotenko I.V. Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems // IOP Conference Series: Materials Science and Engineering. 2020. V. 709. P. 033034. https://doi.org/10.1088/1757-899X/709/3/033034
10. Сухопаров М.Е., Семенов В.В., Лебедев И.С. Мониторинг информационной безопасности элементов киберфизических систем с использованием искусственных нейронных сетей // Методы и технические средства обеспечения безопасности информации. 2018. № 27. С. 59–60.
11. Шелухин О.И., Осин А.В. Мультифрактальные свойства трафика реального времени // Электротехнические и информационные комплексы и системы. 2006. Т. 2. № 3. С. 36–43.
12. Semenov V., Sukhoparov M., Lebedev I. An approach to classification of the information security state of elements of cyber-physical systems using side electromagnetic radiation // Lecture Notes in Computer Science. 2018. V. 11118. P. 289–298. https://doi.org/10.1007/978-3-030-01168-0_27
13. 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. 2019. V. 11730. P. 703–716. https://doi.org/10.1007/978-3-030-30490-4_56
14. Медведникова М.М. Использование метода главных компонент при построении интегральных индикаторов // Машинное обучение и анализ данных. 2012. Т. 1. № 3. С. 292–304.
15. 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. 2017. V. 10242. P. 88–99. https://doi.org/10.1007/978-3-319-71368-7_8
16. Kravchik M., Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks // Proc. of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy. 2018. P. 72–83. https://doi.org/10.1145/3264888.3264896
17. 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.
18. 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 2017 IEEE International Conference on Data Mining Workshops (ICDMW). 2017. P. 1058–1065. https://doi.org/10.1109/ICDMW.2017.149

References

1. Cardenas A., Amin S., Sinopoli B., Giani A., Perrig A., Sastry S. Challenges for securing cyber physical systems. *Workshop on Future Directions in Cyber-Physical Systems Security*, 2009.
2. Zegzhda D., Vasilev U., Poltavtseva M., Kefele I., Borovkov A. Advanced production technologies security in the era of digital transformation. *Voprosy kiberbezopasnosti*, 2018, no. 2(26), pp. 2–15. (in Russian). https://doi.org/10.21681/2311-3456-2018-2-2-15
3. Semenov V., Salakhutdinova K., Lebedev I., Sukhoparov M. Identification of abnormal functioning during the operation devices of cyber-physical systems. *Journal of Applied Informatics*, 2019, vol. 14, no. 6(84), pp. 114–122. (in Russian). https://doi.org/10.24411/1993-8314-2019-10053
4. Zegzhda D.P. Sustainability as a criterion for information security in cyber-physical systems. *Automatic Control and Computer Sciences*, 2016, vol. 50, no. 8, pp. 813–819. https://doi.org/10.3103/S0146411616080253
5. Pavlenko E.Yu., Shtyrkina A.A., Zegzhda D.P. Estimating the cyber-physical system sustainability based on spectral graph theory. *Information Security Problems*. *Computer Systems*, 2019, no. 1, pp. 60–68. (in Russian)
6. 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
7. Wang X., Zhou Q., Harer J., Brown G., Qiu S., Dou Z., Wang J., Hinton A., Gonzalez C.A., Chin P. Deep learning-based classification and anomaly detection of side-channel signals. *Proceedings of SPIE*, 2018, vol. 10630, pp. 1063006. https://doi.org/10.1117/12.2311329
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. *Lecture Notes in Computer Science*, 2019, vol. 11660, pp. 104–112. https://doi.org/10.1007/978-3-030-30859-9_9
9. Meleshko A.V., Desnitsky V.A., Kotenko I.V. Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems. *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 709, pp. 033034. https://doi.org/10.1088/1757-899X/709/3/033034
10. Sukhoparov M.E., Semenov V.V., Lebedev I.S. Information security monitoring of elements of cyber-physical systems using artificial neural networks. *Metody i Tekhnicheskie Sredstva Obespecheniya Bezopasnosti Informatsii*, 2018, no. 27, pp. 59–60. (in Russian)
11. Osin A.V., Sheluhin O.I. Multifractal properties of the real-time traffic. *Jelektrotehnicheskie i informacionnye kompleksy i sistemy*, 2006, vol. 2, no. 3, pp. 36–43. (in Russian)
12. Semenov V., Sukhoparov M., Lebedev I. An approach to classification of the information security state of elements of cyber-physical systems using side electromagnetic radiation. *Lecture Notes in Computer Science*, 2018, vol. 11118, pp. 289–298. https://doi.org/10.1007/978-3-030-01168-0_27
13. 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*, 2019, vol. 11730, pp. 703–716. https://doi.org/10.1007/978-3-030-30490-4_56
14. Medvednikova M.M. Principal component analysis for building integral indicators. *Machine Learning and Data Analysis*, 2012, vol. 1, no. 3, pp. 292–304. (in Russian)
15. 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*, 2017, vol. 10242, pp. 88–99. https://doi.org/10.1007/978-3-319-71368-7_8
16. Kravchik M., Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks. *Proc. of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, 2018, pp. 72–83. https://doi.org/10.1145/3264888.3264896
17. 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.
18. 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 2017 IEEE International Conference on Data Mining Workshops (ICDMW)*, 2017, pp. 1058–1065. https://doi.org/10.1109/ICDMW.2017.149

19. 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. 2021. in press. https://doi.org/10.1109/TDSC.2021.3050101
20. 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

19. 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*, 2021, in press. https://doi.org/10.1109/TDSC.2021.3050101
20. 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

Автор

Семенов Виктор Викторович — 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 — 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 13.09.2021
Одобрена после рецензирования 01.11.2021
Принята к печати 28.11.2021

Received 13.09.2021
Approved after reviewing 01.11.2021
Accepted 28.11.2021