

ПОВЫШЕНИЕ КАЧЕСТВА АНАЛИЗА СОСТОЯНИЯ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ ПРИ СЕГМЕНТАЦИИ СЕТЕВОГО ТРАФИКА

Лебедев Илья Сергеевич,
Санкт-Петербургский федеральный исследовательский
центр Российской академии наук, Санкт-Петербург,
Россия, isl_box@mail.ru

Сикарев Игорь Александрович,
Российский государственный гидрометеорологический
университет, Санкт-Петербург, Россия,
sikarev@yandex.ru

Сухопаров Михаил Евгеньевич,
Российский государственный гидрометеорологический
университет, Санкт-Петербург, Россия,
mail@sukhoparovm.ru

Рзаев Бабыр Темирбекулы,
Казахский агротехнический университет
им. С. Сейфуллина, г. Нур-Султан, Республика Казахстан,
pathinchaos@gmail.com

Рассматривается актуальная задача выявления аномальных ситуаций, возникающих в информационно-телекоммуникационных системах (ИТКС), при помощи методов искусственного интеллекта. Анализ процессов функционирования устройств и узлов ИТКС в реальных условиях показывает, что с течением времени свойства анализируемых характеристик могут трансформироваться. Различные факторы вызывают смещение диапазонов анализируемых значений целевых переменных. Появление в различные моменты времени внешних и внутренних событий изменяют состояния как отдельных телекоммуникационных устройств, так и системы в целом. Необходимо проводить анализ большого числа разнородных качественных и количественных характеристик трафика и процессов функционирования телекоммуникационных устройств. Предлагаемый метод мониторинга состояния ИТКС основывается на учете факторов, влияющих на изменение свойств целевых переменных, что, в свою очередь, позволяет осуществлять сегментацию выборки данных. Новизна предлагаемого решения заключается в том, что для отдель-

ных сегментов обрабатываемых данных применяется алгоритм классификации, имеющий лучшие качественные показатели. Учитывая текущие и предполагаемые ситуации, возможно сформировать выборки на основе выявленных воздействий. На основе датасета NSL-KDD осуществляется сегментация множества данных, учитывающая влияния факторов на диапазоны значений. Показана обработка факторов с помощью функции поиска разладки временного ряда, с помощью которой осуществлялась сегментация набора данных. В результате сегментации данных было получено конечное число непересекающихся измеримых подмножеств данных, каждое из которых подавалось на вход алгоритму классификации. Произведена оценка качества работы классификационных алгоритмов. На основе полученных результатов возможно построение различных моделей классификации состояния информационной безопасности (ИБ) ИТКС. Предложенный подход позволяет повысить качественные показатели алгоритмов классификации в динамически меняющихся условиях.

Ключевые слова: анализ состояния, информационно-телекоммуникационные системы, мониторинг состояния, алгоритм классификации, сегментация данных, деревья решений, метод опорных векторов

Информация об авторах:

Лебедев Илья Сергеевич, д.т.н., профессор, Заведующий лабораторией интеллектуальных систем Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия

Сикарев Игорь Александрович, д.т.н., профессор, Заведующий кафедры Морских информационных систем Федерального государственного бюджетного образовательного учреждения высшего образования "Российский государственный гидрометеорологический университет", Санкт-Петербург, Россия

Сухопаров Михаил Евгеньевич, д.т.н., Доцент кафедры Морских информационных систем Федерального государственного бюджетного образовательного учреждения высшего образования "Российский государственный гидрометеорологический университет", Санкт-Петербург, Россия

Рзаев Бабыр Темирбекулы, Аспирант кафедры Информационных систем Казахского агротехнического университета им. С. Сейфуллина, г. Нур-Султан, Республика Казахстан

Для цитирования:

Лебедев И.С., Сикарев И.А., Сухопаров М.Е., Рзаев Б.Т. Повышение качества анализа состояния безопасности телекоммуникационной системы при сегментации сетевого трафика // Т-Comm: Телекоммуникации и транспорт. 2022. Том 16. №9. С. 28-32.

For citation:

I. Lebedev, I. Sikarev, M. Sukhoparov, B.T. Rzayev (2022). Improving the quality of telecommunications system security state analysis during network traffic segmentation. *T-Comm*, vol. 16, no.9, pp. 28-32. (in Russian)

DOI: 10.36724/2072-8735-2022-16-9-28-32

Manuscript received 06 July 2022;
Accepted 28 July 2022

Введение

Развитие, повсеместное использование ИТКС обуславливает лавинообразный рост трафика, который необходимо обрабатывать и анализировать. В зависимости особенностей информационных систем трафик может обладать различными свойствами, определяемыми объемом, частотой служебных и информационных сообщений. Архитектура и структура ИТКС дает возможность разбить его на отдельные составляющие, где в каждом сегменте последовательности сообщений и пакетов будут обладать своими свойствами.

Представление сетевого трафика в виде моделей, основанных на дискретных состояниях, позволяют использовать методы машинного обучения для выявления и идентификации деструктивных воздействий, которые могут возникать в системе.

Однако очень часто в течение времени при работе информационной системы может происходить изменение диапазонов, смена распределений выходных и входных данных.

Достижение заданных показателей при определении деструктивных воздействий связано не только с методами машинного обучения, но и со свойствами данных в выборках. Учитывая постоянные изменения диапазонов значений целевых переменных, свойств обрабатываемых данных, появляется дополнительная задача адаптации методов машинного обучения.

Существующие подходы

Возможности достижения заданных качественных показателей алгоритмами классификации зависят от свойств обрабатываемых данных. Наличие шумов, ошибок, выбросов данных в обучающих выборках обычно приводит к потере полноты, точности реализуемой модели обработки. В ряде работ, например [1-5], исследуются зависимости качественных показателей различных алгоритмов классификации от свойств данных. Наличие данных, повторяющих свойства генеральной совокупности, во многих случаях важнее алгоритма классификации, что вызывает необходимость создания репрезентативных выборок.

Повышение качества моделей машинного обучения достигается применением различных подходов и направлений.

Первое связано с решениями, использующими комбинации разнородных классифицирующих алгоритмов, обученных на отдельных множествах данных [6-9]. Такие модели направлены на создание ансамблей классифицирующих алгоритмов, объединяющих и обобщающих результаты. Однако они не являются универсальными, трудно интерпретируемы, не имеют общепринятых правил для включения в свой состав того или иного классификатора.

В основе второго направления применяются методы анализа изменений в распределении вероятностей. Они направлены на анализ диапазонов значений характеристик поступающего потока данных и обнаружение изменений их свойств. Подобные решения являются ресурсоемким, и, в случае трансформации свойств данных, возникает необходимость дополнительных операций настройки для достижения заданной точности [10-12].

Третье направление – модели прогнозного анализа поведения данных [10,13-15]. Их разработка требует предварительной обработки, направленной на определение свойств различных характеристик объектов наблюдения и их изменений в течение времени. Увеличение количества анализируемых целевых переменных значительно повышают вычислительные затраты и сложность модели.

Рассматриваемые подходы, в основном, требуют существенных затрат на адаптацию и реализацию [14,15]. Однако они являются универсальными и могут быть применены для ИТКС.

В условиях функционирования информационно-телекоммуникационных систем возникает задача заранее определить и обосновать метод, алгоритм, обеспечивающий заданное качество решения. В результате применяются различные комбинации. Выбор модели обработки данных обосновывается значениями функционала качества на контрольных подвыборках данных.

В рассматриваемой статье предлагается учесть факторы, влияющих на свойства трафика путем решения задачи сегментации выборки данных и сформировать стратегию, определяющую назначение классификатора на сегмент выборки.

Предлагаемый подход

В задачах машинного обучения основным проблемным вопросом остается формирование выборок данных. На практике возникают ситуации, когда в ходе функционирования ИТКС изменяются свойства трафика. Например, в зависимости от количества абонентов в сети происходит изменение объема в дневные и ночные часы. Разнородность признакового пространства, при формировании которого учитываются различные сообщения и их внутренняя структура, влечет за собой дополнительные сложности для алгоритмов классификации. Одинаковые сообщения, имеющие различные флаги, указывают на возникновение разных событий в сети. Одновременно с этим по мере функционирования системы могут происходить изменения диапазонов и распределений исследуемых переменных.

В подобных условиях качественные показатели алгоритмов классификации сильно зависят от репрезентативности набора данных для сетевого трафика.

Кортеж значений $X = (x_1, \dots, x_n)$, характеризующий сетевой трафик, имеет множество параметров. В ходе функционирования системы в течение определенного момента времени может увеличиваться частота как информационных, так и служебных сообщений с различными флагами. Например, появление относительно большого количества сообщений конфигурации сети, может говорить о возможной попытке подключения к сети. А это, в свою очередь, дает информацию для того, чтобы определить легальность данных попыток.

На основе количественных характеристик, используя размеченную выборку, основанную на «историческом» опыте, возможно определить нормальное и аномальное состояние.

Обозначим $\{c_1, c_2\} = c$ метки нормального и аномального состояния ИТКС.

Количественные значения атрибутов x_1, \dots, x_n являются предикторами, на основе анализа значений которых, необходимо наиболее точно соотнести конкретный объект c к своей группе – нормальному c_1 или аномальному c_2 состоянию.

В таком случае идентификация состояния ИТКС рассматривается как задача машинного обучения, определенная в компактном пространстве X и меток c , предполагающая создание алгоритма:

$$\mu: X \rightarrow c. \quad (1)$$

В целях определения качественных показателей классификатора μ (1) возможно определить функцию потерь L , которая сравнивает прогноз с меткой.

Анализ состояния ИТКС можно рассмотреть как классификационную задачу. Для выборки X^p (где p – количество кортежей выборки) измерение потерь алгоритма классификации $\mu(x_i)$, определяется с помощью индикатора ошибок:

$$I(x, \mu) = [\mu(x_i) \neq c_j]. \quad (2)$$

Анализ потерь возможно осуществить на основе частоты ошибок (2) алгоритма $\mu(x)$:

$$L(\mu, X^p) = \frac{1}{p} \sum_{i=1}^p I(\mu(x_i), c_j). \quad (3)$$

Диапазоны переменных изменяются под воздействием факторов V . Они могут быть определены явно. Например, рабочее и нерабочее время, может оказывать существенное влияние на объем сетевого трафика. Однако ввиду возможного одновременного воздействия не всегда удастся однозначно их интерпретировать, что приводит к необходимости анализа выборки данных автоматическими методами, например, поиска разладки сигнала или обнаружения дрейфа концепта [16].

Влияние внешних и внутренних факторов на ИТКС приводит к тому, что выборка данных становится неоднородной, а неоднородности возникают в результате воздействия факторов.

Для повышения качественных показателей методов машинного обучения, на которые влияют выбросы данных, шумы, изменения плотности вероятности возникновения событий необходимо разбивать множество X^p на подмножества с учетом влияния на данные факторов $v_i \in V, i = 1, \dots, m$:

$$X^p = X_1^{p1} \cup X_2^{p2} \cup \dots \cup X_m^{pm}, \sum_{i=1}^m p_i = p. \quad (4)$$

Тогда для каждого подмножества $X_i^{pi} \in X^p$, где действует фактор или их совокупность v_i необходимо минимизировать функцию потерь:

$$L_i(\mu_i, X_i^{pi}) \rightarrow \min. \quad (5)$$

Использование заранее выбранных алгоритмов классификации $a_i \in A$, на основании выражения (4) дает возможность определить для каждого сегмента X_i^{pi} тот классификатор, который имеет лучшие значения функции потерь.

Потери на всей выборке необходимо минимизировать используя различные заранее предопределенные на каждом сегменте классификаторы.

$$\sum_{i=1}^m L_i(\mu_i, X_i^{pi}) \rightarrow \min. \quad (6)$$

Применение выражения (6) на каждом сегменте выборки позволяет выбрать группу классификаторов, где каждый из

них, имеет наилучшие показатели на предопределенном ему сегменте.

Экспериментальная оценка

С целью оценки предлагаемого решения для проведения эксперимента был взят набор данных NSL-KDD. В выборке NSL-KDD Test содержится 22544 записей, из них 9711 с классом нормального, 12833 аномального трафика. Выборка была разделена на две части – обучающую и тестовую. Структура данных содержит более 40 значений атрибутов [17].

В первой части эксперимента проводилась сегментация с использованием библиотеки “ruptures”. Выделенные точки разладки временного ряда представлены на рисунке 1.

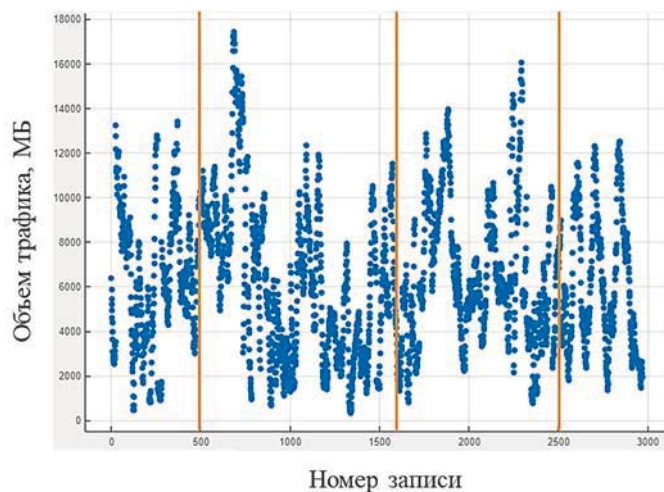


Рис. 1. Определение точек изменения и границ сегментирования в многомерном представлении, по горизонтальной оси представлено время (time), по вертикальной оси объем данных (volume), передаваемых от источника к пункту назначения в одном соединении

В результате сетевой трафик был разбит на несколько сегментов. Каждый из которых имеет свои свойства, связанные с трендом и статистическим размахом данных. На всех полученных сегментах было произведено обучение классификаторов DT, SVM и для каждого из них определены значения показателей.

Рассматривая требуемый показатель качества и используя выражение (5) можно выбрать тот классификатор, который покажет лучшие значения на сегменте, т.е. назначить на конкретный сегмент свой классификатор.

На рисунке 2 представлены показатели по всей выборке целиком, по сегментам, и средние значения, полученные при выборе наилучших классификаторов.

Анализ гистограмм показывает, что, используя сегментацию выборки и назначая классификаторы, имеющие лучшие показатели качества, возможно повысить качество обработки всей выборки.

Таким образом, сегментация множества данных позволяет бороться с выбросами, формировать компактно локализованные подмножества в пространстве объектов. Используя сегментацию, можно повысить качественные показатели приблизительно на 5% по сравнению с выборкой в целом. Тем не менее, качественные показатели моделей напрямую зависят от свойств данных, на основе которых происходит процесс обучения и тестирования.

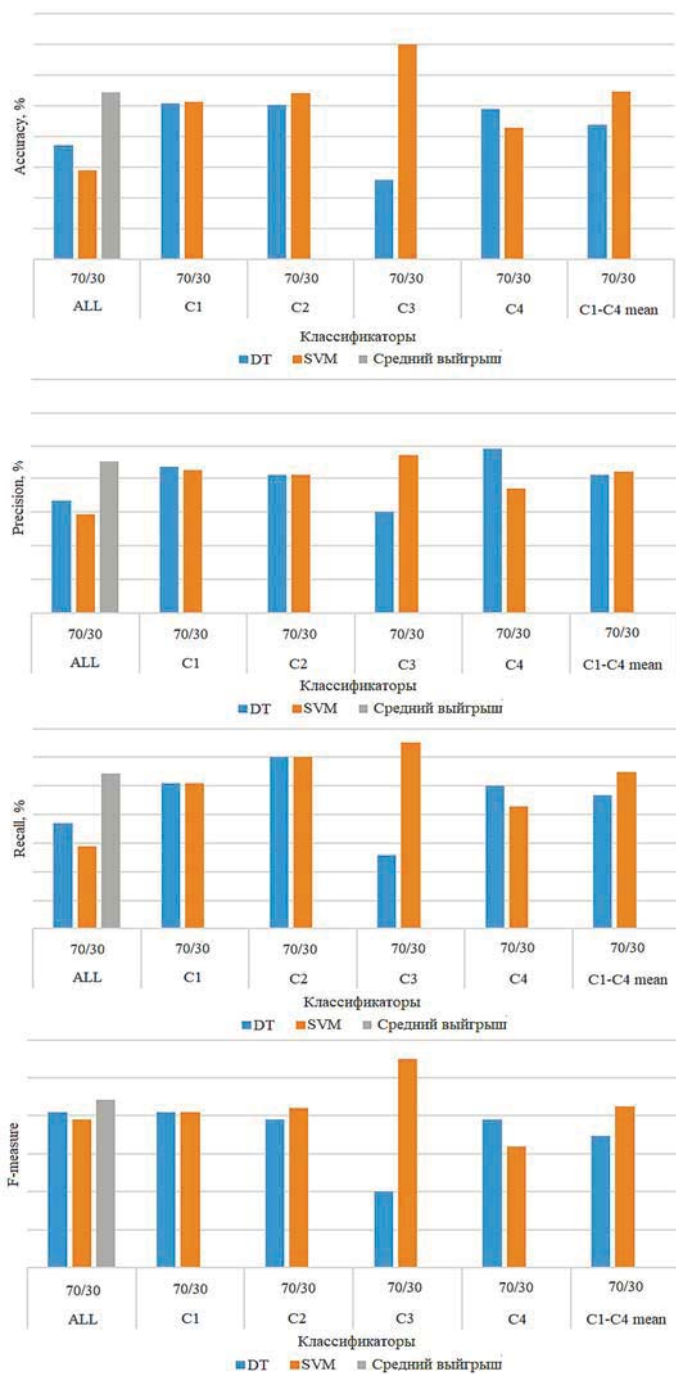


Рис. 2. Качественные показатели классификации

Выводы

В статье предложено решение, основанное на применении заранее обученных и предопределенных классификаторов для анализа состояния ИТКС. В основе метода лежит разделение выборки на отдельные сегменты, с отличающимися свойствами данных.

В ряде случаев возможно заранее определить факторы, которые влияют на различные свойства трафика, а это позволяет осуществлять сегментацию значений. В результате становится возможным выделение отдельных сегментов, обладающих однородными свойствами, на которыми применяется имеющий лучшие качественные показатели классифицирующий алгоритм.

Такой подход позволяет не строить сложных разделяющих поверхностей на всей совокупности данных, а выбирать классифицирующий алгоритм на сегменте. Это дает возможность снизить вычислительные затраты при обработке данных, использовать простые, хорошо интерпретируемые модели, быстро их переучивать в случае возникновения трансформации свойств данных.

Предложенный метод можно использовать как дополнение к различным классификационным моделям. Однако для его эффективной реализации необходимо проводить предварительный этап, направленный на оценку свойства данных при различных воздействующих факторах.

Литература

1. *Ruoxi Jia*. Efficient task-specific data valuation for nearest neighbor algorithms // Proceedings of the VLDB Endowment, 2019. Vol. 12.11. P. 1610-1623.
2. *Deng, Z., Zhu, X., Cheng, D., Zong, M., & Zhang, S*. Efficient kNN classification algorithm for big data // Neurocomputing, 2016. Vol. 195. P. 143-148.
3. *Maillo, J., Ramirez, S., Triguero, I., & Herrera, F*. kNN-IS: An Iterative Spark-based design of the k-Nearest Neighbors classifier for big data // Knowledge-Based Systems, 2017. Vol. 117. P. 3-15.
4. *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.
5. *Kaftannikov I.L., Parasich A.V.* Problems of training set's formation in machine learning tasks // Bulletin of the South Ural State University. Series Computer Technology, Automatic Control, Radio Electronics, 2016. Vol. 16, no. 3. P. 15-24.
6. *Fanaee T. H., Gama J*. Event labeling combining ensemble detectors and background knowledge // Progress in Artificial Intelligence, 2014. Vol. 2. P. 113-127.
7. *Bishop C.M., Nasser M.N.* Pattern recognition and machine learning. Journal of Electronic Imaging, 2007. Vol. 16. P. 49-69.
8. *Sukhoparov M.E., Semenov V.V., Salakhutdinova K.I., Boitsova E.P., Lebedev I.S.* The state identification of Industry 4.0 mechatronic elements based on behavioral patterns. Internet of Things, Smart Spaces, and Next Generation Networks and Systems // Proc. of 20th Intern. Conf., NEW2AN, and 13th Conf., ruSMART, 2020. No. 1. P. 126-134.
9. *Sethi T., Kantardzic M*. Handling adversarial concept drift in streaming data Expert Systems with Applications, 2018. Vol. 97. P. 18-40.
10. *Lebedev I.S.* Dataset segmentation considering the information about impact factors // Information and Control Systems, 2021. Vol. 3. P. 29-38.
11. *Saadallah A., Moreira-Matias L., Sousa R., Khiari J., Jenelius E., Gama J*. Bright-drift-aware demand predictions for taxi networks // IEEE Transactions on Knowledge and Data Engineering, 2020. Vol. 32. P. 234-245.
12. *Gomes H. M., Bifet A., Read J., Barddal J. P., Enembreck F., Pfahringer B., Holmes G*. Adaptive random forests for evolving data stream classification // Machine Learning, 2017. Vol. 106, no. 9-10. P. 1469-1495.
13. *Семенов В.В., Лебедев И.С., Сухопаров М.Е.* Идентификация состояния информационной безопасности беспилотных транспортных средств с использованием искусственных нейронных сетей // Методы и технические средства обеспечения безопасности информации: Материалы 28-й научно-технической конференции, 2019. № 28. С. 46-47.
14. *Takacs A., Toledano-Ayala M., Dominguez-Gonzalez A., Pastrana-Palma A., Velazquez D.T., Ramos J.M., Rivas-Araiza A.E.* Descriptor generation and optimization for a specific outdoor environment // IEEE Access, 2020. Vol. 8. P. 2169-2182.
15. *Maletzke A., dos Reis D., Cherman E., Batista G.* DyS: A Framework for Mixture Models in Quantification // Proceedings of the AAAI Conference on Artificial Intelligence, 2019. Vol. 33, no 1. P. 4552-4560.
16. *Lebedev I.S.* Various machine learning models application on separate segments in regression and classification problems // Information and Control Systems, 2022. No. 3. P.9-19
17. *Bhupendra I., Anamika Y.* Performance Analysis of NSL-KDD dataset using ANN // International Conference on Signal Processing and Communication Engineering Systems (SPACES), 2015. P. 92-96.

IMPROVING THE QUALITY OF TELECOMMUNICATIONS SYSTEM SECURITY STATE ANALYSIS DURING NETWORK TRAFFIC SEGMENTATION

Ilya Lebedev, Saint-Petersburg federal research center of Russian science academy, Saint-Petersburg, Russia, isl_box@mail.ru

Igor Sikarev, Marine information systems department, Russian State Hydrometeorological University, Saint-Petersburg, Russia, sikarev@yandex.ru

Mikhail Sukhoparov, Marine information systems department, Russian State Hydrometeorological University, Saint-Petersburg, Russia, mail@sukhoparovm.ru

Babyr Temirbekuly Rzayev, S.Seifullin Kazakh Agro Technical University, Nur-Sultan, Republic of Kazakhstan, pathinchaos@gmail.com

Abstract

The article deals with the actual task of identifying abnormal situations arising in information and telecommunication systems (ITCS) using artificial intelligence methods. Analysis of the processes of functioning of ITCS devices and nodes in real conditions shows that over time the properties of the analyzed characteristics can be transformed. Various factors cause the ranges of the analyzed values of the target variables to shift. The appearance of external and internal events at various points in time changes the states of both individual telecommunication devices and the system as a whole. It is necessary to analyze a large number of heterogeneous qualitative and quantitative characteristics of traffic and processes of functioning of telecommunication devices. The proposed method of monitoring the state of ITCS is based on taking into account the factors influencing the change in the properties of target variables, which, in turn, allows segmentation of the data sample. The novelty of the proposed solution lies in the fact that a classification algorithm with the best quality indicators is used for individual segments of the processed data. Taking into account the current and expected situations, it is possible to form samples based on the identified impacts. On the basis of the NSL-KDD dataset, segmentation of the data set is carried out, taking into account the influence of factors on the ranges of values. The processing of factors using the search function of the time series layout, which was used to segment the data set, is shown. As a result of data segmentation, a finite number of non-overlapping measurable subsets of data were obtained, each of which was fed to the classification algorithm. The evaluation of the quality of the classification algorithms was carried out. Based on the results obtained, it is possible to build various classification models of the ITCS information security (IS) status. The proposed approach makes it possible to improve the quality indicators of classification algorithms in dynamically changing conditions.

Keywords: state analysis, information and telecommunication systems, state monitoring, classification algorithm, data segmentation, decision trees, support vector machine.

References

1. Ruoxi Jia. (2019). Efficient task-specific data valuation for nearest neighbor algorithms. *Proceedings of the VLDB Endowment*. Vol. 12.11, pp. 1610-1623.
2. Deng Z., Zhu X., Cheng D., Zong M., & Zhang S. (2016). Efficient kNN classification algorithm for big data. *Neurocomputing*. Vol. 195, pp. 143-148.
3. Maillo J., Ramirez, S., Triguero I., & Herrera F. (2017). kNN-IS: An Iterative Spark-based design of the k-Nearest Neighbors classifier for big data. *Knowledge-Based Systems*. Vol. 117, pp. 3-15.
4. Sukhoparov M.E., Semenov V.V., Salakhutdinova K.I., Lebedev I.S. (2020). Detection of abnormal functioning of Industry 4.0 devices based on behavioral patterns. *Information Security Problems. Computer Systems*. Vol. 1 (41), pp. 96-102. (in Russian)
5. Kaftannikov I.L., Parasich A.V. (2016). Problems of training set's formation in machine learning tasks. *Bulletin of the South Ural State University. Series Computer Technology, Automatic Control, Radio Electronics*. Vol. 16, no. 3, pp. 15-24.
6. Fanaee T. H., Gama J. (2014). Event labeling combining ensemble detectors and background knowledge. *Progress in Artificial Intelligence*. Vol. 2, pp. 113-127.
7. Bishop C.M., Nasser M.N. (2007). Pattern recognition and machine learning. *Journal of Electronic Imaging*. Vol. 16, pp. 49-69.
8. Sukhoparov M.E., Semenov V.V., Salakhutdinova K.I., Boitsova E.P., Lebedev I.S. (2020). The state identification of Industry 4.0 mechatronic elements based on behavioral patterns. Internet of Things, Smart Spaces, and Next Generation Networks and Systems: *Proc. of 20th Intern. Conf., NEW2AN, and 13th Conf., ruSMART*. No. 1, pp. 126-134.
9. Sethi T., Kantardzic M. (2018). Handling adversarial concept drift in streaming data Expert Systems with Applications. Vol. 97, pp. 18-40.
10. Lebedev I.S. (2021). Dataset segmentation considering the information about impact factors. *Information and Control Systems*. Vol. 3, pp. 29-38.
11. Saadallah A., Moreira-Matias L., Sousa R., Khiari J., Jenelius E., Gama J. (2020). Bright-drift-aware demand predictions for taxi networks. *IEEE Transactions on Knowledge and Data Engineering*. Vol. 32, pp. 234-245.
12. Gomes H. M., Bifet A., Read J., Barddal J. P., Enembreck F., Pfahringer B., Holmes G. (2017). Adaptive random forests for evolving data stream classification. *Machine Learning*. Vol. 106, no. 9-10, pp. 1469-1495.
13. Semenov V. V., Lebedev I. S., Sukhoparov M. E. (2019). State identification of information security of unmanned vehicles using artificial neural networks. *Methods and information security engineering: Proceedings of the 28th Scientific and Technical Conference*. Vol. 28, pp. 46-47. (in Russian)
14. Takacs A., Toledano-Ayala M., Dominguez-Gonzalez A., Pastrana-Palma A., Velazquez D.T., Ramos J.M., Rivas-Araiza A.E. (2020). Descriptor generation and optimization for a specific outdoor environment. *IEEE Access*. Vol. 8, pp. 2169-2182.
15. Maletzke A., dos Reis D., Cherman E., Batista G. (2019). DyS: A Framework for Mixture Models in Quantification. *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 33, no 1, pp. 4552-4560.
16. Lebedev I.S. (2022). Various machine learning models application on separate segments in regression and classification problems. *Information and Control Systems*. No. 3, pp. 9-19.
17. Bhupendra I., Anamika Y. (2015). Performance Analysis of NSL-KDD dataset using ANN. *International Conference on Signal Processing and Communication Engineering Systems (SPACES)*, pp. 92-96.

Information about authors:

Ilya Lebedev, Head of Intelligent systems laboratory, Saint-Petersburg federal research center of Russian science academy, Saint-Petersburg, Russia

Igor Sikarev, Head of the department, Marine information systems department, Russian State Hydrometeorological University, Saint-Petersburg, Russia

Mikhail Sukhoparov, Associate professor, Marine information systems department, Russian State Hydrometeorological University, Saint-Petersburg, Russia

Babyr Temirbekuly Rzayev, Postgraduate student of the Information systems Department, S.Seifullin Kazakh Agro Technical University, Nur-Sultan, Republic of Kazakhstan