УДК 004.056
DOI: 10.26102/2310-6018/2023.40.1.002

Обеспечение целостности телеметрической информации о состоянии сложного технического объекта

А.И. Фрид, А.М. Вульфин✉, М.Б. Гузаиров, В.В. Берхольц

Уфимский университет науки и технологий, Уфа, Российская Федерация
vulfin.alexey@gmail.com✉

Резюме. Актуальность исследования обусловлена необходимостью повышения защищенности передаваемой на предприятие-изготовитель телеметрической информации, позволяющей анализировать состояние бортовых подсистем, возникающие сбои и неисправности, а также обнаруживать возможные воздействия злоумышленника. На основе алгоритмов предиктивной аналитики телеметрической информации могут быть выявлены неисправности и предотказные состояния бортовых подсистем и системы автоматического управления газотурбинным двигателем летательного аппарата. Оперативный сбор и анализ телеметрии позволяет специалистам наземных технических служб планировать ремонтные и профилактические мероприятия. Накапливаемая в течение длительного периода телеметрия позволяет непрерывно адаптировать цифровые модели подсистем, блоков и модулей летательного аппарата, с использованием которых возможна значимая поддержка принятия решений в случае технического сбоя. В связи с этим, целью работы является повышение вероятности выявления несанкционированной модификации передаваемых данных телеметрии о состоянии сложного технического объекта – системы автоматического управления газотурбинным двигателем. Основным методом исследования данной проблемы является интеллектуальный анализ многомерных временных рядов параметров, характеризующих состояние бортовых систем летательного аппарата. В статье разработана структура системы мониторинга целостности телеметрической информации, передаваемой с борта летательного аппарата, основанная на анализе согласованности многомерных временных рядов. Выполняется сравнение телеметрии с борта летательного аппарата и выходов цифровой модели сложного технического изделия. На выходе системы формируется оценка вероятности нарушения целостности переданных на предприятие-изготовитель данных. Материалы статьи представляют практическую ценность для повышения уровня защиты информации при ее передаче с борта летательного аппарата на предприятие-изготовитель.

Ключевые слова: телеметрическая информация, интеллектуальный анализ, многомерные временные ряды, ансамбль нейросетевых классификаторов, параметры согласованности временных рядов.

Благодарности: работа выполнена при поддержке гранта РФФИ № 20-08-00668.

Для цитирования: Фрид А.И., Вульфин А.М., Гузаиров М.Б., Берхольц В.В. Метод обеспечения целостности телеметрической информации о состоянии сложного технического объекта. *Моделирование, оптимизация и информационные технологии.* 2023;11(1). URL: https://moitvivt.ru/ru/journal/pdf?id=1289 DOI: 10.26102/2310-6018/2023.40.1.002

Ensuring the integrity of telemetric information on the state of a complex technical object

A.I. Frid, A.M. Vulfin✉, M.B. Guzairov, V.V. Berkholts

Ufa University of Science and Technology, Ufa, Russian Federation
vulfin.alexey@gmail.com✉

Abstract. The relevance of the study is due to the need to improve the security of telemetry information transmitted to the manufacturer, which allows analyzing the state of on-board subsystems, failures and malfunctions, as well as detecting possible intruder impacts. On the basis of algorithms for predictive analytics of telemetric information, malfunctions and pre-failure states of on-board subsystems, and automatic control systems for the gas turbine engine of an aircraft can be detected. Efficient collection and analysis of telemetry helps specialists of ground technical services to plan repair and preventive measures. Telemetry accumulated over a long period makes it possible to continuously adapt digital models of aircraft subsystems, blocks and modules, which can be used to provide significant decision support in the event of a technical failure. In this regard, the purpose of the research is to increase the probability of detecting unauthorized modification of the transmitted telemetry data on the state of a complex technical object – a gas turbine engine automatic control system. The main method for studying this problem is the intellectual analysis of multidimensional time series of parameters characterizing the state of the onboard systems of the aircraft. The article develops the structure of the system for monitoring the integrity of telemetric information transmitted from the aircraft based on the analysis of the consistency of multidimensional time series. A comparison is made between telemetry from the aircraft and the outputs of a digital model of a complex technical product. At the output of the system, the probability estimate of integrity violation of the data transmitted to the manufacturer is formed. The materials of the article are of practical value for increasing the level of information protection when it is being transmitted from the aircraft to the manufacturer.

Keywords: telemetry information, intellectual analysis, multidimensional time series, ensemble of neural network classifiers, time series consistency parameters.

Acknowledgments: the reported research was supported by the RFBR grant No. 20-08-00668.

For citation: Frid A.I., Vulfin A.M., Guzairov M.B., Berkholts V.V. Ensuring the integrity of telemetric information on the state of a complex technical object. *Modeling, Optimization and Information Technology*. 2023;11(1). URL: https://moitvivt.ru/ru/journal/pdf?id=1289 DOI: 10.26102/2310-6018/2023.40.1.002 (In Russ.).

Введение

Современные подходы мониторинга состояния газотурбинных двигателей летательных аппаратов (ГТД ЛА) реализуют существенно более сложные математические модели и позволяют учитывать нестационарность процессов, характеризующих состояние сложных технических объектов, в условиях ограниченного набора измеряемых параметров, неточности и неполноты получаемых данных о состоянии наблюдаемого объекта [1, 2].

Цифровые системы управления ГТД включают механизмы контроля и диагностики состояния на основе собираемых с датчиков подсистем ЛА данных. Собираемая телеметрия через канал «борт-наземные службы» передается на предприятие-изготовитель (ПИ) для повышения оперативности принятия решений при возникновении нештатных ситуаций и решении задач предиктивной аналитики.

Актуальной является [3-8] проблема ограниченных вычислительных ресурсов бортовых систем контроля и диагностики. Решение проблемы возможно за счет передачи накапливаемых данных о состоянии системы автоматического управления (САУ) ГТД в наземные информационные системы ПИ с последующей обработкой с помощью технологий интеллектуального анализа.

В ходе сбора, обработки и хранения данных может быть нарушена их целостность из-за вмешательства внутренних и внешних злоумышленников. Анализ систем «борт-наземные службы» показал, что наиболее распространенные на сегодняшний день системы являются уязвимыми, и злоумышленник может получить доступ к системе управления полетом [6]. Следовательно, необходима разработка систем, способных выявлять нарушение целостности телеметрической информации (ТМИ), передаваемой

через информационно-телекоммуникационные сети на ПИ. Система мониторинга реализует непрерывный анализ и выявление значимых отклонений в работе САУ ГТД от наземной цифровой модели, что указывает на возможные нарушения целостности передаваемых данных. Анализ согласованности модельных данных и данных с борта ЛА позволяет выявлять отклонения от «нормального» режима работы ГТД, реализуя концепцию Fault Detection and Identification [9-13].

В работе [14] рассмотрена система, реализующая мониторинг целостности ТМИ, получаемой с ЛА о состоянии САУ ГТД, и передаваемых с борта ЛА на предприятие-изготовитель. Применяется сравнение технологических временных рядов (ТВР), характеризующих поведение параметров САУ ГТД, установленной на ЛА, и модели САУ ГТД, установленной на ПИ, по показателям: коэффициент корреляции и детерминации и средний процент отклонения. Для принятия решения о модификации ТМИ злоумышленником используется анализ сигнала системы контроля исправности САУ ГТД и режима работы САУ ГТД. Недостатком системы является низкая вероятность обнаружения вмешательства злоумышленника, обусловленная применением алгоритмов автоматической классификации и использованием только лишь двух метрик оценок согласованности ТВР, основанных на определении дисперсии.

В работах [15, 16] представлен способ и система мониторинга целостности данных, получаемых с эксплуатируемой САУ ГТД ЛА. Способ основан на применении алгоритмов адаптивной сегментации ТВР с использованием таких характеристик сигналов, как: амплитуда, форма волны (морфологии), длительность, распределение энергии, частотное содержание и т. д., с последующей идентификацией фрагментов ТВР и сопоставлением их с отдельными событиями. Блок принятия решений о наличии вмешательства злоумышленника (модификации информации, передаваемой с борта ЛА на ПИ) определяет режим работы САУ ГТД (установившийся или переходный) и выполняет сравнение получаемых данных с результатами моделирования на ПИ.

Недостатками представленных решений являются:

– наличие подсистемы, выполняющей классификацию режимов работы САУ ГТД на установившийся и переходный, что повышает вычислительную сложность принятия решения о модификации данных злоумышленником за счет необходимости введения двух типов классификаторов с различной архитектурой;

– избыточная структура гетерогенного классификатора на основе нейро-нечетких сетей, решающая задачу определения типа согласованности, когда основной интерес представляет решение бинарной задачи классификации о наличии или отсутствии модификации данных злоумышленником;

– вычислительная сложность нейро-нечетких моделей как на этапе построения гетерогенного классификатора, так и на этапе его эксплуатации ввиду отсутствия эффективной программной и / или программно-аппаратной реализации;

– недостаточно высокая вероятность обнаружения вмешательства злоумышленника, обусловленная тем, что в ходе анализа используется сравнение только одной пары ТВР параметров, получаемых с борта ЛА, и генерируемых моделью на ПИ; для оценки согласованности пары ТВР (данных, полученных с борта ЛА, и модельных данных) используются метрики, не учитывающие возможные временные сдвиги и масштабирование сравниваемых подпоследовательностей ТВР.

Следовательно, целью исследования является повышение вероятности выявления несанкционированной модификации передаваемых на предприятие-изготовитель данных телеметрии о состоянии системы автоматического управления газотурбинным двигателем. Для достижения поставленной цели необходима разработка системы

мониторинга целостности передаваемой телеметрии на основе технологий интеллектуального анализа многомерных временных рядов.

Система мониторинга целостности телеметрической информации

Проектируемая система мониторинга состояния САУ ГТД ЛА основана на сопоставлении выходов цифровой модели САУ ГТД [17-23] и ТМИ с борта ЛА. Анализ целостности данных ТМИ основан на выделении в результирующем сигнале, характеризующем согласованность модельных и натурных данных, аномалий и скрытых закономерностей.

Предлагаемый способ мониторинга целостности данных, получаемых с эксплуатируемой САУ ГТД ЛА, основан на применении методов интеллектуального анализа многомерных технологических временных рядов параметров, характеризующих состояние ГТД, с использованием алгоритма адаптивного скользящего окна [24] и оценки параметров согласованности ТВР. Блок принятия решений о состоянии канала передачи с борта ЛА на ПИ обеспечивает обработку ТВР, характеризующих работу САУ ГТД ЛА, и производит их сравнение с данными моделирования на ПИ.

Структурная схема способа мониторинга целостности данных САУ ГТД летательного аппарата представлена на Рисунке 1, основные обозначения представлены в Таблице 1.

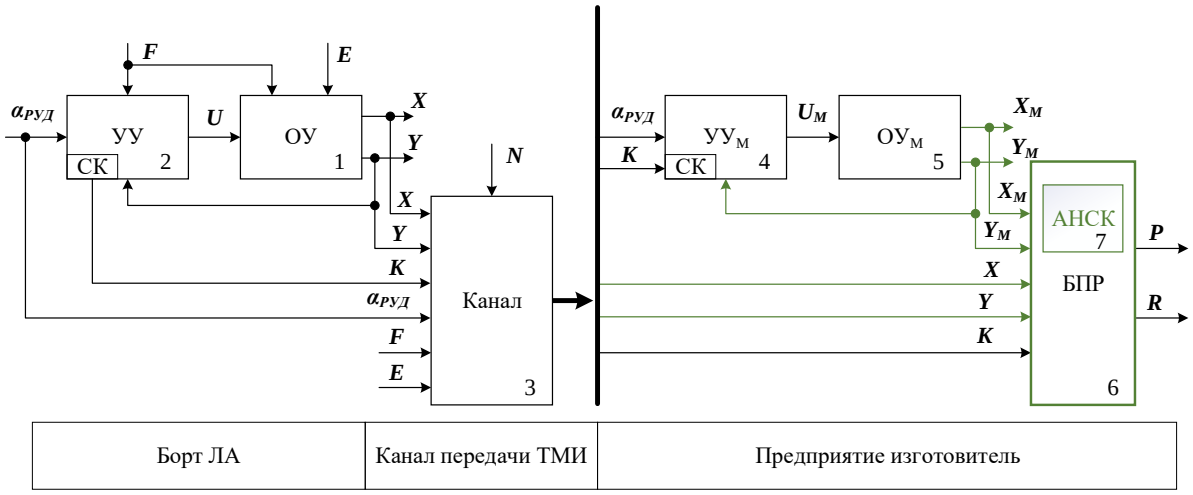

Рисунок 1 – Структурная схема способа мониторинга целостности данных, получаемых с бортовых систем летательного аппарата
Figure 1 – Structural diagram of the method for monitoring the integrity of data received from on-board systems of an aircraft

Таблица 1 – Основные обозначения схемы способа мониторинга целостности данных, получаемых с бортовых систем летательного аппарата
Table 1 – Basic designations diagram of the method for monitoring the integrity of data received from on-board systems of an aircraft

№	Обозначение параметра	Параметр	Примечания
1	*F*	свойства внешней среды, такие как параметры атмосферного воздуха: температура за бортом ЛА, давление и прочее	Кортеж

Таблица 1 (продолжение)
Table 1 (extended)

№	Обозначение параметра	Параметр	Примечания
2	E	дополнительные эксплуатационные факторы	Кортеж
3	Y	параметры регулирования, такие как частоты вращения роторов, давление воздуха за компрессором, температура газа за турбиной и т.д.	Кортеж
4	X	характеристики САУ ГТД: тяга, скорость ее изменения, удельный расход топлива и прочее	Кортеж
5	U	кортеж управляющих воздействий, формируемый устройством управления	Кортеж
6	K	сигнал о состоянии САУ ГТД (исправна K=1/неисправна K=0)	Сигнал
7	$\alpha_{РУД}$	положение рычага управления ГТД	Сигнал
8	N	воздействие внешних факторов и шума на канал	Кортеж
9	Y_M	параметры регулирования на выходе модели объекта управления (аналог Y) на предприятии-изготовителе	Кортеж
10	X_M	характеристики модели ГТД (аналог X)	Кортеж
11	U_M	кортеж управляющих воздействий, формируемый моделью устройства управления (аналог UM)	Кортеж

В систему управления ГТД поступают кортежи F и E. Исходящими из объекта управления (ОУ) (1) в составе системы управления на борту ЛА являются кортежи Y и X. В объект управления 1 поступает кортеж управляющих воздействий U, формируемый устройством управления (УУ) (2). Система контроля САУ ГТД формирует сигнал (K) о ее состоянии.

Кортежи X, Y, K, F, E и $\alpha_{РУД}$ передаются через канал передачи данных (3) на предприятие-изготовитель для использования в модели САУ ГТД: блоки (4) и (5). Канал подвергается воздействию внешних факторов и шума (N).

Кортежи X, Y, Y_M, X_M представлены в виде многомерных технологических временных рядов и передаются в результирующий блок принятия решений (БПР) (6), где выполняется оценка их согласованности, а также проверяется состояние сигнала системы контроля (К), затем принимается решение (R) о злонамеренном нарушении целостности данных (произошел отказ оборудования или работа продолжается в штатном режиме), и оценка вероятности правильности принятого решения (P) на основе ансамбля нейросетевых классификаторов (АНСК) (7) передается модульному нейросетевому классификатору.

Способ мониторинга целостности данных, получаемых с борта ЛА, включает следующие основные шаги:

1) формируется набор параметров САУ ГТД для анализа согласованности данных ТМИ, полученных с модели, и данных, полученных с борта ЛА;

2) формируется подпоследовательность многомерных параметров X, Y, Y_M, X_M, X_M^W, X_R^W – наборы ТВР, созданные с помощью модели и полученные с борта ЛА – с помощью адаптивного скользящего окна W_S переменной длины;

3) выполняется расчет параметров согласованности одной, двух и трех пар ТВР (полученных с борта ЛА и генерируемых моделью) для каждой подпоследовательности, попадающей в скользящее окно анализа W_S;

4) строится многомерный технологический временной ряд (мТВР) P_W – параметры согласованности одной, двух и трех пар ТВР для каждой подпоследовательности, попадающей в скользящее окно анализа W_S;

5) на основе параметров согласованности ТВР и сигнала системы контроля принимается решение о целостности данных, полученных с ЛА.

Анализ согласованности многомерных технологических временных рядов ТМИ, порождаемых моделью сложного технического объекта, и данных, получаемых от бортовых систем ЛА, позволяет оценивать условную вероятность нарушения целостности ТМИ. Выходом системы является оценка вероятности наличия подобных событий нарушения целостности.

Отличие предлагаемого способа оценки вероятности наличия атаки, направленной на нарушение целостности принимаемых данных, состоит в том, что кортеж параметров согласованности дополняют параметром соответствия подпоследовательностей сравниваемых технологических временных рядов, определяемым с помощью алгоритма динамической трансформации временной шкалы, вычисляют матрицу трансформации попарно сравниваемых технологических временных рядов, элементами которой являются результаты сравнения одной, двух или трех пар технологических временных рядов, и в соответствии со сформированным кортежем параметров согласованности строят модульную нейросетевую модель, позволяющую обнаруживать факт модификации передаваемых данных и оценивать вероятность подобной модификации, причем кортеж параметров согласованности технологических временных рядов вычисляют на поэтапно выделяемом адаптивном скользящем окне переменной длины, а итоговое решение о состоянии полученных данных принимают на основе трех параметров: тип согласованности одной, двух или трех пар технологических временных рядов, режим работы модели системы автоматического управления газотурбинным двигателем и сигнал системы контроля системы автоматического управления газотурбинным двигателем.

Система, реализующая способ мониторинга целостности данных, получаемых с борта ЛА (Рисунок 2).

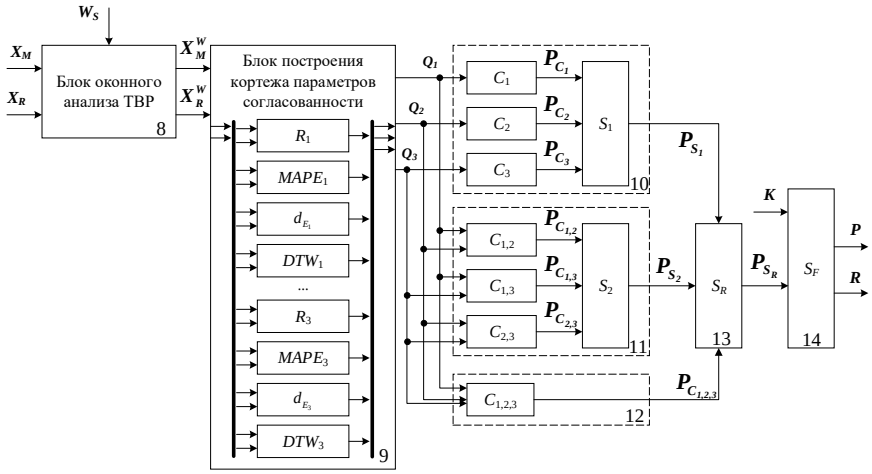

Рисунок 2 – Структурная схема системы, реализующей способ мониторинга целостности данных о состоянии САУ ГТД

Figure 2 – Structural diagram of a system that implements the method for monitoring the integrity of data on the state of a gas turbine engine automatic control system

Блок оконного анализа ТВР (8) с помощью адаптивного скользящего окна длиной W_S с шагом S формирует из исходных многомерных ТВР X_M и X_R набор матриц X_M^W, X_R^W признаков для дальнейшего анализа согласованности ТВР. Размер скользящего окна анализа варьируется в диапазоне от 50 до 250 отсчетов и подбирается на этапе оптимизации параметров моделей-классификаторов экспериментально.

Блок построения кортежа параметров согласованности (9) выполняет построение кортежа PW параметров согласованности трех пар ТВР в текущем окне анализа X_M^W, X_R^W с помощью набора метрик [25, 26]. Метрики оценки включают: коэффициент корреляции (R), среднюю абсолютную ошибку ($MAPE$), Евклидово расстояние (d_E) (Таблица 2).

Таблица 2 – Метрики оценки согласованности многомерных ТВР в текущем окне анализа
Table 2 – Metrics for evaluating the consistency of multidimensional technological time series in the current analysis window

№	Название метрики согласованности	Коэффициент	Параметры
1	Коэффициент корреляции	$r_{xy} = \frac{\sum_{i=1}^{n}\left(x_i - \bar{x}\right)\cdot\left(y_i - \bar{y}\right)}{\left(n-1\right)\cdot S_x \cdot S_y}$	X, Y – две сравниваемые подпоследовательности ТВР равной длины, n – длина подпоследовательностей, $\bar{x}$, $\bar{y}$ – выборочные средние, S_x и S_y выборочные среднеквадратичные отклонения
2	Коэффициент детерминации	$R^2 = r_{xy}^2$	определяется по значению коэффициента корреляции
3	Средняя абсолютная ошибка, %	$MAPE = \frac{1}{n}\sum_{i=1}^{n}\frac{\lvert x_i - y_i\rvert}{x_i}\cdot 100\%$	
4	Евклидово расстояние	$x_{iн} = \frac{x_i - \bar{x}}{S_x}$, $y_{iн} = \frac{y_i - \bar{y}}{S_y}$, $d_E = \sqrt{\sum\left(x_{iн} - y_{iн}\right)^2}$	$\bar{x}$, $\bar{y}$ – выборочные средние величин, S_x и S_y выборочные среднеквадратичные отклонения величин, $x_н$ и $y_н$ – нормированные величины

Дополнительно вводится метрика, определяющая коэффициент оптимального пути трансформации временной шкалы DTW:

$$DTW\left(X,Y\right) = \min_k\left\{\frac{\sum_{k=1}^{K} d\left(w_k\right)}{K}\right\},$$

где d – матрица расстояний, $d\left(x_i, y_j\right) = \left(x_i - y_j\right)^2$,

D – матрица трансформации, $D_{i,j} = d_{i,j} + \min\left(D_{i-1,j}, D_{i-1,j-1}, D_{i,j-1}\right)$,

W – путь трансформации (последовательность смежных элементов матрицы трансформации) длиной $n \le K < 2n$, $w_k = \left(i,j\right)_k$, $d\left(w_k\right) = d\left(x_i, y_j\right) = \left(x_i - y_j\right)^2$.

Расширенный кортеж параметров согласованности пары ТВР используется для последующего принятия решения о возможных причинах выявленных расхождений в блоке принятия решений. Выход блока (9) включает трехкомпонентный кортеж Q_1, Q_2, Q_3 – параметры согласованности для каждой из трех пар анализируемых ТВР.

Первый ансамбль нейросетевых классификаторов (10), второй ансамбль нейросетевых классификаторов (11) и нейросетевой классификатор (12) предназначены для классификации параметров согласованности одной, двух и трех пар ТВР X_M^W, X_R^W. Первый ансамбль нейросетевых классификаторов (10) включает три независимых бинарных классификатора (C_1, C_2, C_3) на основе многослойных полносвязных нейронных сетей прямого распространения, каждый из которых решает задачу классификации параметров согласованности для сравниваемых пар ТВР на два класса: «нормальная работа», «атака». Блок оценки наличия атаки S_1 в составе (10) на основе оценок (P_{C1}, P_{C2}, P_{C3}) вероятности наличия атаки формирует оценку на основе линейной взвешенной комбинации:

$$P_{S_1} = \frac{w_1 \cdot P_{C_1} + w_2 \cdot P_{C_2} + w_3 \cdot P_{C_3}}{w_1 + w_2 + w_3},$$

весовые коэффициенты w_1, w_2, w_3 которой подбираются в процессе построения классификаторов.

Второй ансамбль нейросетевых классификаторов (11) включает три независимых бинарных классификатора ($C_{1,2}$, $C_{1,3}$, $C_{2,3}$) на основе многослойных полносвязных нейронных сетей прямого распространения, каждый из которых решает задачу классификации параметров согласованности для двух сравниваемых пар ТВР на два класса: «нормальная работа», «атака». Блок оценки наличия атаки S_2 в составе 11 на основе оценок (P_{C12}, P_{C13}, P_{C23}) вероятности наличия атаки, формирует оценку P_{S2} на основе линейной взвешенной комбинации, весовые коэффициенты которой также подбираются в процессе построения классификаторов.

Блок нейросетевого классификатора (12) представляет собой бинарный классификатор (C_{123}) на основе многослойной полносвязной нейронной сети прямого распространения, решающий задачу классификации параметров согласованности для трех сравниваемых пар ТВР на два класса: «нормальная работа», «атака».

Блок взвешенной оценки (13) позволяет сформировать взвешенную оценку в виде линейной взвешенной комбинации выходов блоков (10), (11) и (12).

Результирующий блок принятия решения (14) основан на однослойной нейронной сети, реализует принятие решения R о текущем состоянии системы и позволяет произвести оценку вероятности правильности принятого решения P о наличии одного из состояний согласованности данных модели и САУ ГТД: «Отказ САУ ГТД», «Нормальная работа», «Нарушение целостности».

Построение ансамбля нейросетевых классификаторов поясняется с помощью схемы на Рисунке 3.

База данных ($БД_1$) (15) обеспечивает хранение ТМИ в виде двух типов технологических временных рядов: ТВР, полученных с модели, и ТВР, полученных с борта ЛА. ТВР, полученные с борта ЛА, подвергались искажениям: наложению случайного шума и различным сценариям нарушения целостности [15].

Накопленные данные подвергались адаптивному оконному анализу (16), длина скользящего окна W_S и шаг S рассматриваются как оптимизируемые гиперпараметры ансамбля классификаторов и подбираются с помощью поиска по сетке в процессе обучения с использованием алгоритма перекрестной проверки. Все полученные в результате оконного анализа данные накапливаются в базе данных ($БД_2$) (17) в процессе

построения обучающей, тестовой и проверочной выборок (18). Создаются группы бинарных нейросетевых классификаторов для пар ТВР, получаемых с модели САУ ГТД и борта ЛА:

– три классификатора, каждый из которых в качестве входного кортежа признаков использует параметры согласованности Q_1, Q_2 или Q_3 отдельных пар ТВР – C_1 (19);

– три классификатора, каждый из которых в качестве входного кортежа признаков использует параметры согласованности $\left(\{Q_1,Q_2\},\{Q_1,Q_3\},\{Q_2,Q_3\}\right)$ двух пар ТВР – C_2 (20);

– классификатор, в качестве входного кортежа признаков использующий параметры согласованности $\{Q_1,Q_2,Q_3\}$ трех пар ТВР – C_3 (21).

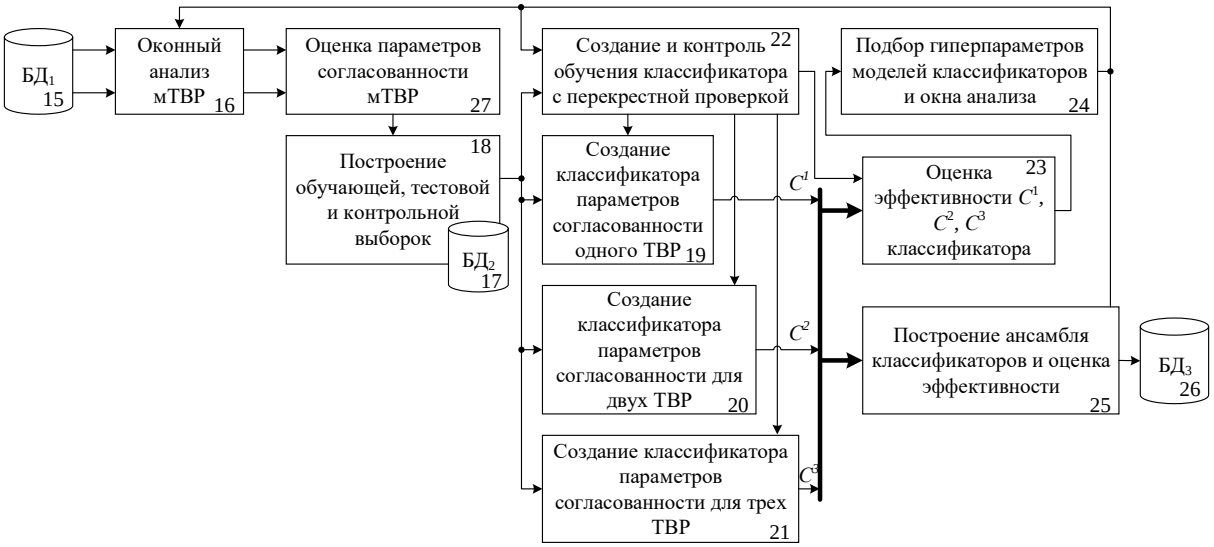

Рисунок 3 – Структурная схема построения ансамблей нейросетевых классификаторов
Figure 3 – Structural scheme for constructing ensembles of neural network classifiers

Блок (22) обеспечивает создание классификаторов и осуществляет контроль и предотвращает переобучение нейросетевых моделей отдельных классификаторов, а также позволяет с помощью алгоритма перекрестной проверки оценить обобщающую способность отдельных классификаторов.

Блок (23) обеспечивает оценку эффективности ансамбля классификаторов на основе подбора коэффициентов линейной взвешенной суммы выходов каждого из классификаторов для параметров согласованности одной, двух и трех ТВР. Блок (24) обеспечивает оптимизацию гиперпараметров ансамбля нейросетевых классификаторов: коэффициентов линейной взвешенной суммы одиночных участников, параметров архитектуры каждой из нейронных сетей, параметров адаптивного оконного анализа исходных ТВР – с помощью алгоритма перебора по сетке.

Блок (25) позволяет оценить качество бинарной классификации ансамбля моделей и сохранить в БД$_3$ (26) весовые коэффициенты и подобранные параметры наилучшего из построенных решений.

В отличие от предыдущих решений [15], выходы блока построения кортежа параметров согласованности технологических временных рядов в виде трехкомпонентного кортежа параметров согласованности связаны с входом первого ансамбля из трех бинарных нейросетевых классификаторов, а также со входом второго

ансамбля из трех бинарных нейросетевых классификаторов и с блоком, реализующим бинарный нейросетевой классификатор, выходы которых связаны с блоком взвешенного суммирования и блоком итоговой оценки вероятности модификации передаваемых данных.

Эксперимент по оценке вероятности успешного распознавания атаки на данные

Тестирование представленного способа проводилось на выборке, включающей ТВР, полученные с модели САУ ГТД, и ТВР, полученные с борта ЛА. На ТВР, полученных с ЛА, накладывался шум, а также симулировались различные случаи нарушения целостности злоумышленником согласно описанной в прототипе методике.

Протокол тестирования включает анализ 11207 подпоследовательностей трех пар тестовых ТВР:

1) G – удельный расход топлива ($ТВР_1$);
2) N – приведенная частота вращения ротора ($ТВР_2$);
3) V – нормированная виброскорость подвески двигателя ($ТВР_3$).

Каждая пара ТВР (ТВР с модели и ТВР, генерируемые САУ ГТД), представляет собой подпоследовательность, попавшую во временное окно, состоящее из W_S отсчетов. На часть данных, полученных с САУ ГТД, были произведены атаки злоумышленника для получения разных типов согласования ТВР. В Таблице 3 показано количество подпоследовательностей, анализируемых $ТВР_1$, $ТВР_2$, $ТРВ_3$, включающих нормальный режим работы САУ ГТД и атаки злоумышленника.

Таблица 3 – Количество подпоследовательностей анализируемых $ТВР_1$, $ТВР_2$, $ТРВ_3$, включающих нормальный режим работы САУ ГТД и атаки злоумышленника
Table 3 – The number of subsequences of the analyzed TVR_1, TVR_2, TRV_3 including the normal operation mode of the gas turbine engine automatic control system and the attacks of an intruder

Наличие атаки по каждому из анализируемых ТВР			Наличие атаки	Количество примеров подпоследовательностей
$ТВР_1$	$ТВР_2$	$ТВР_3$		
1	1	1	1	10925
0	0	0	0	9229
1	0	1	1	1413
	1	0	1	267
0	1	1	1	249
	0	1	1	49

Далее, для каждой пары ТВР вычислялись параметры согласованности и строились нейросетевые классификаторы.

Результаты

Итоговый протокол эксперимента по оценке вероятности успешного распознавания атаки приведен в Таблице 4, из которой видно, что повышение достоверности мониторинга целостности достигается за счет использования свойств связности процессов в ГТД как объекте управления в случае использования двух и трех параметров.

Таблица 4 – Итоговый протокол эксперимента по оценке вероятности успешного распознавания атаки
Table 4 – Final protocol of the experiment on assessing the probability of successful attack recognition

№	Способ	Тестовый ТВР	Оценка вероятности успешного распознавания атаки	Оценка F1 меры успешного распознавания атаки
1	Прототип	$ТВР_1$	0,850	0,820
2	Предложенный способ в случае анализа одной пары ТВР	$ТВР_1$	0,932	0,931
3		$ТВР_2$	0,954	0,950
4		$ТВР_3$	0,946	0,941
5		Взвешенная линейная комбинация	0,945	0,941
6	Предложенный способ в случае анализа двух пар ТВР	$ТВР_1$ и $ТВР_2$	0,951	0,950
7		$ТВР_1$ и $ТВР_3$	0,950	0,950
8		$ТВР_2$ и $ТВР_3$	0,951	0,951
9	Предложенный способ в случае анализа трех пар ТВР	$ТВР_1$, $ТВР_2$, $ТВР_3$	0,954	0,952
10	Предложенный способ в случае анализа трех пар ТВР в виде ансамбля моделей C^1, C^2, C^3	$ТВР_1$, $ТВР_2$, $ТВР_3$	0,962	0,960

Применение для анализа двух параметров принципиально повышает достоверность мониторинга целостности ТМИ. Использование более двух (трех и более) параметров для решения поставленной задачи повышает вероятность принятия правильного решения на очень малую величину и сопровождается существенным повышением требований к вычислительным возможностям системы. На основе результатов эксперимента (Таблица 4), оценка вероятности корректного определения типа согласованности ТВР, а следовательно, и нарушения целостности данных, принятых с борта ЛА, повысилась до 0,962 по сравнению с предыдущим вариантом реализации системы, для которого оценка вероятности составляла 0,850.

Заключение

В статье разработана структура системы мониторинга целостности телеметрической информации, основанная на обнаружении вызванных воздействием возможного злоумышленника аномалий в многомерных временных рядах, полученных с помощью модели сложного технического объекта (САУ ГТД), и принимаемых с бортовых систем летательного аппарата.

Для оценки вероятности наличия атаки, направленной на нарушение целостности принимаемых данных, кортеж параметров согласованности дополнен параметром соответствия подпоследовательностей сравниваемых технологических временных рядов, определяемых с помощью алгоритма динамической трансформации временной шкалы, реализующим построение матрицы трансформации попарно сравниваемых технологических временных рядов, элементами которой являются результаты сравнения

одной, двух или трех пар технологических временных рядов. В соответствии со сформированным кортежем параметров согласованности строится модульная нейросетевая модель, позволяющая обнаруживать факт модификации передаваемых данных и оценивать вероятность подобной модификации, причем кортеж параметров согласованности технологических временных рядов вычисляется на поэтапно выделяемом адаптивном скользящем окне переменной длины, а итоговое решение о состоянии полученных данных принимается на основе трех параметров: тип согласованности одной, двух или трех пар технологических временных рядов, режим работы модели системы автоматического управления газотурбинным двигателем и сигнал системы контроля системы автоматического управления газотурбинным двигателем

Оценка условной вероятности обнаружения событий нарушения целостности данных составила 0,962, что выше на 13 % по сравнению с предложенным ранее решением [15]. Показано, что использование трех и более параметров для решения поставленной задачи повышает вероятность принятия правильного решения лишь незначительно, но сопровождается существенным повышением требований к вычислительным возможностям как наземных, так и бортовых систем.

Таким образом, предложенная система позволяет выявлять несанкционированные воздействия на данные о состоянии САУ ГТД при передаче с борта ЛА на предприятие-изготовитель.

СПИСОК ИСТОЧНИКОВ

1. Васильев В.И., Жернаков С.В. Классификация режимов работы ГТД с использованием технологии нейронных сетей. *Вестник УГАТУ*. 2009;12(1):53–60.
2. Васильев В.И., Жернаков С.В., Муслухов И.И. Бортовые алгоритмы контроля параметров ГТД на основе технологии нейронных сетей. *Вестник УГАТУ*. 2009;12(1):61–74.
3. Боев Н.М., Шаршавин П.В., Нигруца И.В. Построение систем связи беспилотных летательных аппаратов для передачи информации на большие расстояния. *Известия ЮФУ. Технические науки*. 2014;3(152):147–158.
4. Гуревич О.С. и др. Беспроводная демонстрационная система управления ГТД. *Системы автоматического управления авиационными газотурбинными двигателями: Труды ЦИАМ №1346*. 2010:46–58.
5. Bhoopathi Rapolu Internet of aircraft things: an industry set to be transformed. Доступно по: https://aviationweek.com/aerospace/connected-aerospace/internet-aircraft-things-industry-set-be-transformed (дата обращения: 10.12.2022).
6. Hugo Teso Aircraft Hacking. Practical Aero Series. *n.runs Professionals*. 2013. Доступно по: http://conference.hitb.org/hitbsecconf2013ams/materials/ (дата обращения: 10.12.2022).
7. Bandyopadhyay D., Sen J. Internet of things: Applications and challenges in technology and standardization. *Wireless personal communications*. 2011;58(1):49–69.
8. Niggemann O. et al. Data-Driven Monitoring of Cyber-Physical Systems Leveraging on Big Data and the Internet-of-Things for Diagnosis and Control. *DX*. 2015:185–192.
9. Gao W. et al. On SCADA control system command and response injection and intrusion detection. *2010 eCrime Researchers Summit. IEEE*. 2010:1–9.
10. Zhang Y. et al. Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Transactions on Smart Grid*. 2011;2(4):796–808.

11. Bigham J., Gamez D., Lu N. Safeguarding SCADA systems with anomaly detection. *International workshop on mathematical methods, models, and architectures for computer network security. Springer, Berlin, Heidelberg*. 2003:171–182.
12. He Q., Blum R.S. Smart grid monitoring for intrusion and fault detection with new locally optimum testing procedures. *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2011:3852–3855.
13. Kim M. et al. Design of a steady-state detector for fault detection and diagnosis of a residential air conditioner. *International journal of refrigeration*. 2008;31(5):790–799.
14. Guzairov M.B. et al. The concept of integrity of telemetric information about the state of an aircraft power plant monitoring. *2019 International Conference on Electrotechnical Complexes and Systems (ICOECS). IEEE*. 2019:1–6.
15. Фрид А.И., Вульфин А.М., Берхольц В.В. Способ мониторинга целостности телеметрической информации о состоянии двигателя летательного аппарата. *Безопасность информационных технологий*. 2020;27(4):65–76.
16. Фрид А.И., Вульфин А.М., Берхольц В.В. Патент № 2740544 С1 Российская Федерация, МПК G06F 21/31. Способ и система мониторинга целостности данных: № 2020122967: опубл. 15.01.2021.
17. Frid A.I. et al. Architecture of the security access system for information on the state of automatic control systems of aircraft. *Acta Polytechnica Hungarica*. 2020;17(8):151–164.
18. Frid A.I., Vulfin A.M., Berkholts V.V. Analysis of the methods of constructing information attack models for the system of telemetric information transmission. *Информационные технологии интеллектуальной поддержки принятия решений (ITIDS'2018)*. 2018:226–229.
19. Frid A.I. et al. The architecture of the web application for protected access to the informational system of processing critically important information. *Computer Science and Information Technologies (CSIT'2017)*. 2017:16–22.
20. Guzairov M.B. et al. Simulation modelling of the transmission system of the telemetric information on the status of the on-board aircraft status. *Data Science. IV International Conference on Information Technology and Nanotechnology*. 2018:105–111.
21. Berkholts V.V. et al. The structure of secure system for collection, storage and processing of telemetric information on the state of aircraft subsystems. *Industrial 4.0*. 2018;3(4):209–212.
22. Гузаиров М.Б. и др. Защищенный доступ к базе данных о состоянии систем автоматического управления (САУ) авиационными ГТД через веб-приложение. *Информация и безопасность*. 2017;20(3):410–413.
23. Гвишиани А.Д. Нечеткие сравнения и распознавание аномалий на временных рядах. *Кибернетика и системный анализ*. 2008;44(3):3–18.
24. Ярушкина Н.Г., Афанасьева Т.В., Перфильева И.Г. *Интеллектуальный анализ временных рядов: учебное пособие.* Ульяновск: УлГТУ; 2010. 320 с.
25. Armstrong J.S., Collopy F. Error measures for generalizing about forecasting methods: Empirical comparisons. *International journal of forecasting*. 1992;8(1):69–80.
26. Загоруйко Н.Г. *Прикладные методы анализа данных и знаний*. Новосибирск: ИМ СО РАН; 1999. 270 с.

REFERENCES

1. Vasilyev V.I., Zhernakov S.V. Classification of gas turbine engine operating modes using neural network technology. *Vestnik UGATU*. 2009;12(1):53–60. (In Russ.).

2. Vasilyev V.I., Zhernakov S.V., Musluhov I.I. On-board algorithms for control of gas turbine engine parameters based on neural networks technology. *Vestnik UGATU*. 2009;12(1):61–74. (In Russ.).
3. Boev N.M., Sharshavin P.V., Nigruca I.V. Building communication systems for unmanned aerial vehicles for transmitting information over long distances. *Izvestiya JuFU. Tehnicheskie nauki.* 2014;3(152):147–158. (In Russ.).
4. Gurevich O.S. et al. Wireless demo GTE control system. *Sistemy avtomaticheskogo upravlenija aviacionnymi gazoturbinnymi dvigateljami: Trudy CIAM №1346*. 2010:46–58. (In Russ.).
5. Bhoopathi Rapolu Internet of aircraft things: an industry set to be transformed. Available by: https://aviationweek.com/aerospace/connected-aerospace/internet-aircraft-things-industry-set-be-transformed (accessed on 10.12.2022).
6. Hugo Teso Aircraft Hacking. Practical Aero Series. *n.runs Professionals*. 2013. Available by: http://conference.hitb.org/hitbsecconf2013ams/materials/ (accessed on 10.12.2022).
7. Bandyopadhyay D., Sen J. Internet of things: Applications and challenges in technology and standardization. *Wireless personal communications*. 2011;58(1):49–69.
8. Niggemann O. et al. Data-Driven Monitoring of Cyber-Physical Systems Leveraging on Big Data and the Internet-of-Things for Diagnosis and Control. *DX*. 2015:185–192.
9. Gao W. et al. On SCADA control system command and response injection and intrusion detection. *2010 eCrime Researchers Summit. IEEE*. 2010:1–9.
10. Zhang Y. et al. Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Transactions on Smart Grid*. 2011;2(4):796–808.
11. Bigham J., Gamez D., Lu N. Safeguarding SCADA systems with anomaly detection. *International workshop on mathematical methods, models, and architectures for computer network security. Springer, Berlin, Heidelberg*. 2003:171–182.
12. He Q., Blum R.S. Smart grid monitoring for intrusion and fault detection with new locally optimum testing procedures. *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2011:3852–3855.
13. Kim M. et al. Design of a steady-state detector for fault detection and diagnosis of a residential air conditioner. *International journal of refrigeration*. 2008;31(5):790–799.
14. Guzairov M.B. et al. The concept of integrity of telemetric information about the state of an aircraft power plant monitoring. *2019 International Conference on Electrotechnical Complexes and Systems (ICOECS). IEEE*. 2019:1–6.
15. Frid A.I., Vulfin A.M., Berkholts V.V. The method of aviation gas turbine engine state information integrity monitoring. *Bezopasnost Informatsionnykh Tekhnologiy*. 2020;27(4):65–76. (In Russ.).
16. Frid A.I., Vulfin A.M., Berkholts V.V. Patent № 2740544 C1 Russian Federation, MPK G06F 21/31. Method and system for monitoring data integrity: № 2020122967: publ. 15.01.2021 (In Russ.).
17. Frid A.I. et al. Architecture of the security access system for information on the state of automatic control systems of aircraft. *Acta Polytechnica Hungarica*. 2020;17(8):151–164.
18. Frid A.I., Vulfin A.M., Berkholts V.V. Analysis of the methods of constructing information attack models for the system of telemetric information transmission. *Proceedings of the 6th All-Russian Scientific Conference Information Technologies for Intelligent Decision Making Support (ITIDS'2018)*. 2018:226–229.
19. Frid A.I. et al. The architecture of the web application for protected access to the informational system of processing critically important information. *Computer Science and Information Technologies (CSIT'2017)*. 2017:16–22.

20. Guzairov M.B. et al. Simulation modelling of the transmission system of the telemetric information on the status of the on-board aircraft status. *Data Science. IV International Conference on Information Technology and Nanotechnology*. 2018:105–111.
21. Berkholts V.V. et al. The structure of secure system for collection, storage and processing of telemetric information on the state of aircraft subsystems. *Industrial 4.0*. 2018;3(4):209–212.
22. Guzairov M.B. et al. Secure access to the database on the state of automatic control systems (ACS) of aircraft gas turbine engines through a web application. *Informacija i bezopasnost*. 2017;20(3):410–413. (In Russ.).
23. Gvishiani A.D. Fuzzy Comparisons and Anomaly Recognition in Time Series. *Kibernetika i sistemnyj analiz*. 2008;44(3):3–18. (In Russ.).
24. Jarushkina N.G., Afanas'eva T.V., Perfileva I.G. *Time Series Mining: a Tutorial.* Uljanovsk: UlGTU; 2010. 320 p. (In Russ.).
25. Armstrong J.S., Collopy F. Error measures for generalizing about forecasting methods: Empirical comparisons. *International journal of forecasting*. 1992;8(1):69–80.
26. Zagorujko N.G. *Applied methods of data and knowledge analysis*. Novosibirsk: IM SO RAN; 1999. 270 p. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Фрид Аркадий Исаакович, доктор технических наук, профессор Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: frid46@mail.ru

Arkady Isaakovich Frid, Doctor of Technical Sciences, Professor at Ufa University of Science and Technology, Ufa, Russian Federation.

Вульфин Алексей Михайлович, кандидат технических наук, доцент Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: vulfin.alexey@gmail.com
ORCID: 0000-0001-5857-2413

Alexey Mikhailovich Vulfin, Candidate of Technical Sciences, Associate Professor at Ufa University of Science and Technology, Ufa, Russian Federation.

Гузаиров Мурат Бакеевич, доктор технических наук, профессор Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: guzairov@ugatu.su

Murat Bakeevich Guzairov, Doctor of Technical Sciences, Professor at Ufa University of Science and Technology, Ufa, Russian Federation.

Берхольц Виктория Викторовна, старший преподаватель Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: torina4@yandex.ru

Victoria Viktorovna Berkholts, Senior Lecturer at Ufa University of Science and Technology, Ufa, Russian Federation.

Статья поступила в редакцию 11.12.2022; одобрена после рецензирования 10.01.2023; принята к публикации 20.01.2023.

The article was submitted 11.12.2022; approved after reviewing 10.01.2023; accepted for publication 20.01.2023.