УДК 004.056

СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛИЙ СОСТОЯНИЯ КИБЕРФИЗИЧЕСКИХ ОБЪЕКТОВ В ЗАДАЧЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е. А. Атарская[1], А. М. Вульфин[2], Л. Я. Узбекова[3]

[1] atarskaya.ea@ugatu.su, [2] vulfin.alexey@gmail.com, [3] uzbekova.lya@ugatu.su

ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ)

Аннотация. В статье представлен алгоритм анализа технологических временных рядов и гетерогенная модель детекторов обнаружения аномалий, вызванных воздействием злоумышленника, пытающегося перехватить управление или навязать алгоритм управления киберфизическим объектом. Предлагаемый подход направлен на совершенствование механизмов предиктивного анализа в составе систем обнаружения и устранения аномалий производственных и технологических процессов АСУ ТП.

Ключевые слова: кибефизические системы; система обнаружения аномалий; аномалии; нейронные сети; технологические временные ряды; автоэнкодеры; длительная кратковременная память.

ВВЕДЕНИЕ

На современном этапе цифрой трансформации индустрии особенно актуальным являются вопросы поддержание работоспособности киберфизических систем (КФС) – обеспечение устойчивости физических процессов и непрерывности управления в условиях целенаправленных внутренних и внешних деструктивных воздействий. Основное направление развития систем защиты информации для обеспечения устойчивости КФС – реализация опережающей стратегии защиты (проактивная защита), основанной на предсказании угрозы (предиктивный анализ) и раннем обнаружении атаки с возможностью адаптации системы к предполагаемому деструктивному воздействию.

В концепции расширенного обнаружения и устранения угроз важная роль отводится предиктивному анализу, являющемуся одним из методов обеспечения киберустойчивости системы. Методы предиктивного анализа направленны на выявление предвестников неполадок и сбоев функционирования, ведущих к деградации киберфизических объектов в составе КФС, на основе анализа накапливаемых параметров их состояния. Основным инструментом предиктивного анализа является выявление аномалий во временных рядах накапливаемых параметров состояния КФО. Под аномалией понимается отклонение в функционировании киберфизического объекта или отклонения и нарушение взаимодействия устройств при обмене данными в составе КФО [1].

АНАЛИЗ СИСТЕМ ОБНАРУЖЕНИЯ АНОМАЛИЙ В РАМКАХ КОНЦЕПЦИИ РАСШИРЕННОГО ОБНАРУЖЕНИЯ И УСТРАНЕНИЯ УГРОЗ КИБЕРБЕЗОПАСНОСТИ

При построении систем обнаружения аномалий в задачах обеспечения киберустойчивости КФС возникает необходимость сбора и обработки значительных объемов, структурированных и слабоструктурированных данных со всех уровней КФС для формирования набора параметров, пригодных для оперативного анализа и выявления аномалий, возникающих в результате воздействий злоумышленника. Ключевую роль при решении этой задачи играют методы интеллектуального анализа данных (ИАД) и методы машинного обучения.

Функциональная модель интеллектуального анализа временных рядов параметров, характеризующих состояние КФО, в задаче обнаружения аномалий с точки зрения группы разработчиков информационно-аналитических систем (ИАС) (рисунок 1).

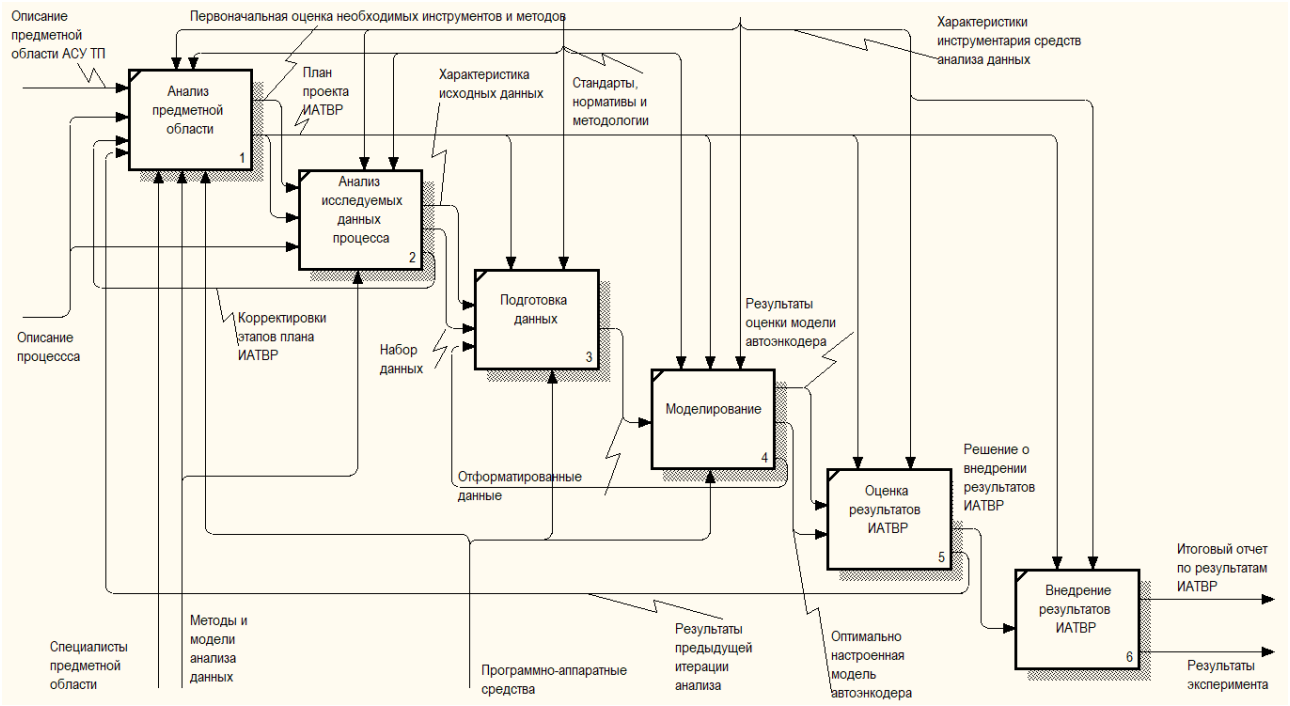

Рис. 1. Функциональная модель процесса ИАД ВР.

АНАЛИЗ КИБЕРФИЗИЧЕСКОГО ОБЪЕКТА И НАБЛЮДАЕМЫХ ПАРАМЕТРОВ

Предложенный исследователями *Institute of ETRI, Daejeon, South Korea* в [2, 3] набор данных собран в ходе эксплуатации стендовой АСУ ТП и дополнен результатами программно-аппаратного моделирования генерации энергии паровой турбиной и процесса гидроаккумулирования. Целью создания является исследование методов и алгоритмов обнаружения аномалий в таких киберфизических системах, как: паровые турбины, водоочистные сооружения и электростанции. Первоначально запущены три испытательных стенда: стенд турбины *General Electronics*, стенд паровых котлов *Emerson* и стенд *MPS FESTO* для водоочистки. Затем построена система, которая объединила три стенда с программно-аппаратным симулятором (*HIL*), который имитирует выработку тепловой и гидроаккумулирующей энергии. Первая версия набора данных содержит нормальные и аномальные ситуации, соответствующие 34 сценариям атак [3].

Технологические процессы на испытательном стенде показаны на рисунке 2:

- процесс котла (*P1*),
- процесс турбины (*P2*),
- процесс водоподготовки (*P3*);
- *HIL*-моделирование (*P4*) сценариев выработки тепловой энергии и генерации гидроаккумулирования энергии.

Процессы котла и турбины используются для моделирования тепловой электростанции, а процесс очистки воды используется для моделирования гидроаккумулирующей электростанции.

Было проведено 50 атак, включая 25 примитивов атак и 25 комбинированных атак одновременного выполнения сразу двух примитивов атаки. Сценарии атак реализуются с учетом цели атаки, времени атаки и метода для каждого контура управления с обратной связью.

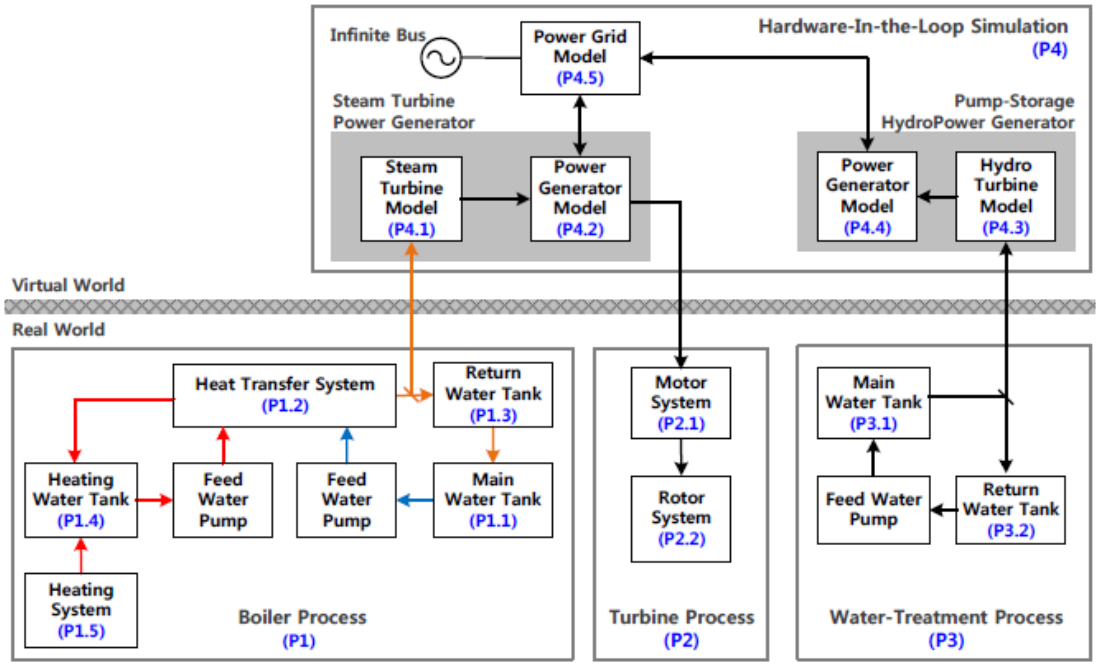

Рис.2. Технологическая схема анализируемого стенда

РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЙ АНОМАЛИЙ В НАБЛЮДАЕМЫХ ПАРАМЕТРАХ СОТОЯНИЯ КИБЕРФИЗИЧЕСКОГО ОБЪЕКТА

Структурная схема системы обнаружения аномалий технологического процесса, основанная на применении методов анализа собираемых данных телеметрии, и позволяющая выявить действия злоумышленника, получившего доступ в промышленную сеть управления технологическим процессом, представлена на рисунке 3.

Технологические временные ряды представляют собой последовательность измерений, собранных с датчиков промышленных объектов. Во временных рядах аномалии представляют собой отрезки временного ряда. На этапе предварительной обработки входные данные подвергаются нормализации и фильтрации. С помощью метода скользящего окна из временных рядов набора данных формируются обучающие и тестовые выборки [4].

Для создания детектора аномалий используются данные о нормальной деятельности для построения модели нормального поведения. Обучающая выборка содержит только данные о нормальном поведении системы, тестовая – содержит данные и нормального класса, и класса аномалий (одиночные атаки и их комбинации).

В данном исследовании применяется несколько алгоритмов для построения моделей машинного обучения с целью обнаружения аномалий. Выбраны следующие модели:

- детектор на основе нейросетевого автоэнкодер *LSTM* для одномерного и многомерного ТВР,
- детектор выбросов с автоподстойкой порога (*LOF*-детектор),
- детектор аномалий на основе изолирующего леса (*IFO*-детектор),
- детектор аномалий на основе машины опорных векторов (*One-class SVM*).

Нейросетевой автоэнкодер в задаче обнаружения аномалий предназначен для восстановления (реконструкции) фрагмента ТВР. Обнаружение аномалий основано на пороговом сравнении среднеквадратической (или абсолютной) ошибки между фактическими данными и восстановленным образом.

Применяемая архитектура НС на основе долгой краткосрочной памяти (*LSTM*) является особой разновидностью архитектуры рекуррентных нейронных сетей, способной к анализу долговременных зависимостей.

Основным преимуществом моделей автоэнкодеров в задаче обнаружения аномалий является возможность построения модели нормального поведения системы. При появлении новых типов аномалий или изменении характера текущих аномалий детектор на основе автоэнкодера, по-прежнему, оценивая ошибку реконструкции образа, способен выявлять подобные образы [5].

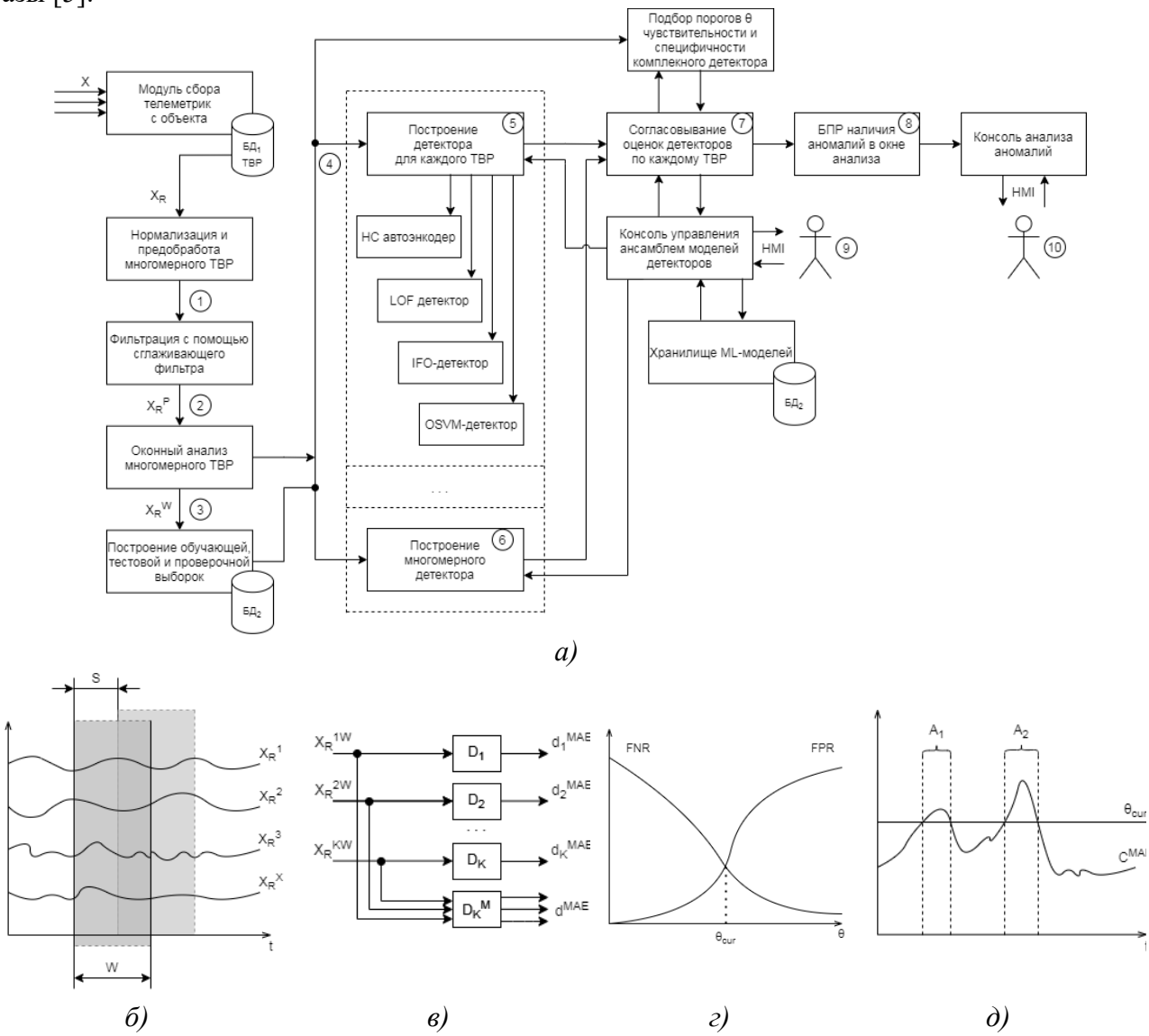

Рис.3. Структурная схема системы обнаружения аномалий (*а*); процесс формирования с помощью скользящего окна фрагментов многомерного ТВР (*б*); многомерный нейросетевой детектор (*в*); подбор порогового значения для определения аномального окна анализа (*г*); визуализация разметки аномальных фрагментов ТВР на основе порогового сравнения ошибки восстановления образа с помощью детектора (*д*).

На рисунке 3 использованы следующие обозначения:

X_R – нормализация каждого из рядов многомерного ТВР (1);

X_R^P – сглаженные многомерные ТВР (2);

X_R^W – скользящее окно длины W с шагом S формирует набор отсчетов для анализа по каждому из рядов ТВР (рисунок 7, б)) (3);

подготовленные данные для построения, тестирования и использования ансамбля детекторов (4);

комитет автоэнкодеров на основе нейронной сети LSTM (5). Детектор выбросов с автоподстройкой порога (LOF детектор). Детектор аномалий на основе модели изолирующего леса (IFO). Детектор аномалий на основе машины опорных векторов (One class SVM).

многомерный детектор НС LSTM (см. рисунок 7, в);

суммирование оценок детекторов в каждом окне *W* одномерных ТВР (7);
блок принятия решений о наличии аномалий в окне анализа *W* одномерных ТВР (8);
специалист по интеллектуальному анализу данных (9);
оператор системы обнаружения аномалий (10).

Итоговая модель ансамбля детекторов для обнаружения аномалий в многомерном технологическом временном ряду, характеризующем ход технологического процесса, включает группу детекторов для одномерных ТВР и детектор для многомерного ТВР на основе нейросетевых автоэнкодеров, *LOF* и *IFO* моделей (рисунок 4).

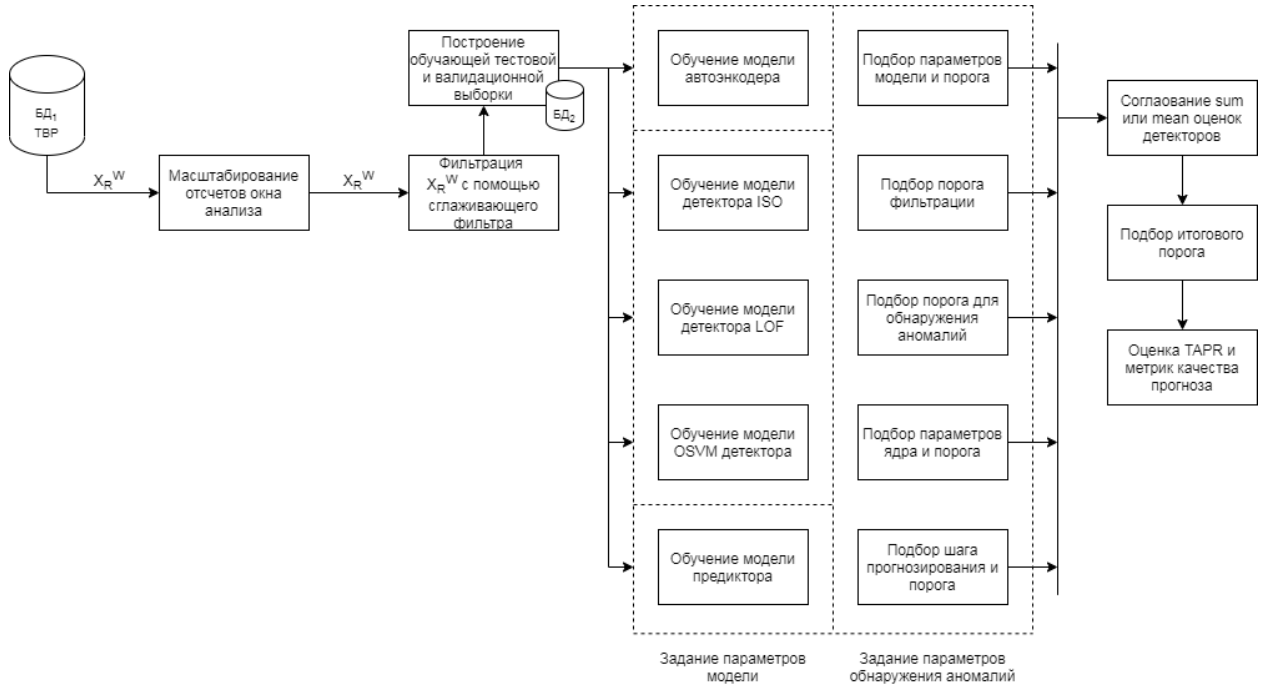

Рис. 4. Модель обнаружения аномалий на основе ансамбля детекторов.

ЭКСПЕРИМЕНТ НА НАТУРНЫХ ДАННЫХ

Описание полей набора данных. Обучающая выборка содержит 921603 примеров без аномалий (атаки не проводились, штатный режим работы системы) и 309604 примеров тестовых данных с тремя типа одиночных и комбинированных атак. Применяется нормализация количественных признаков – приведение к нулевому среднему и единичному стандартному отклонению, и выполняется преобразование категориальных переменных в количественные.

Корреляционная матрица исходных временных рядов. С помощью попарной корреляции Пирсона для переменных обучающей выборки построена тепловая карта, позволяющая оценить параметры с сильной линейной зависимостью. Удаление зависимых переменных позволит существенно ускорить обучение моделей обнаружения аномалий.

Генерация оконных признаков для классификаторов. Скользящее окно длиной 90 отсчетов (экспертная оценка, являющаяся компромиссом для обнаружения длительных и кратковременных аномалий) с шагом 1 перемещается по каждому из ТВР 28 признаков.

Исходный набор данных без дополнительных признаков, рассчитанных для скользящих окон:

- выходной вектор – *'attack', 'attack_P1', 'attack_P2', 'attack_P3'*
- входной вектор – отсчеты 28 временных рядов
- в обучающей выборке содержится 921514 примеров, в тестовой – 309604 примеров.

Таблица 1

Сводная таблица оценки качества работы детектора по обнаружению аномалий

	Все атаки		Первая атака		Вторая атака		Третья атака	
	f1-score	*support*	*f1-score*	*support*	*f1-score*	*support*	*f1-score*	*support*
0	0.97	1224315	0.97	1225819	0.97	1229746	0.97	1230487
1	0.13	6770	0.10	5266	0.03	1339	0.02	598
accuracy	0.95	1231085	0.95	1231085	0.95	1231085	0.95	1231085
macro avg	0.55	1231085	0.54	1231085	0.50	1231085	0.49	1231085
weighted avg	0.97	1231085	0.97	1231085	0.97	1231085	0.97	1231085
F_beta(0,5)	0.9835		0.9847		0.9882		0.9888	

ЗАКЛЮЧЕНИЕ

Для выявления атак необходимы методы и инструменты расширенной аналитики данных, позволяющие выполнять оперативный анализ и выявление скрытых признаков злонамеренной активности на основе модели наблюдаемого КФО.

Для построения модели обнаружения аномалий состояния КФО, вызванных действиями злоумышленника в промышленной сети в ходе реализации сложной сетевой атаки, использован набор данных [3], который собран в ходе испытаний АСУ ТП и дополнен результатами программно-аппаратного моделирования.

Разработана структурная схема системы обнаружения аномалий технологического процесса, основанная на применении методов анализа собираемых данных телеметрии, и позволяющая выявить действия злоумышленника, получившего доступ в промышленную сеть управления технологическим процессом.

В результате реализации алгоритмов анализа данных для сегмента сети АСУ ТП получена оценка эффективности предложенного решения на натурных данных. Обнаружение аномалий по всем типам составило в среднем 65 % (первого типа – 69 %, второго типа – 78 %, третьего типа – 80 %).

СПИСОК ЛИТЕРАТУРЫ

1. Зегжда Д. П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. – М.: Горячая ЛинияТелеком, 2020. – 560 с.

2. Shin H. K. et al. {HAI} 1.0: HIL-based Augmented {ICS} Security Dataset / 13th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 20). – 2020.

3. HAI Security Dataset | Kaggle [Электронный ресурс]. – Режим доступа: https://www.kaggle.com/icsdataset/hai-security-dataset

4. Соболев К.В. Автоматический поиск аномалий во временных рядах. Магистерская диссертация / Соболев Константин Викторович – Москва, 2018.

5. João Pereira Unsupervised Anomaly Detection in Time Series Data using Deep Learning / – 2018.

ОБ АВТОРАХ

АТАРСКАЯ Елена Андреевна, студент 1-курса магистратуры
ВУЛЬФИН Алексей Михайлович, доцент кафедры вычислительной техники и защиты информации
УЗБЕКОВА Лилия Явгаровна, преподаватель кафедры вычислительной математики и кибернетики

METADATA

Title: Anomaly detection system for cyber physical objects in the information security problem.
Affiliation Ufa University of Science and Technology (UUST), Russia.
Email: [1] atarskaya.ea@ugatu.su, [2] vulfin.alexey@gmail.com, [3] uzbekova.lya@ugatu.su
Language: Russian.
Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa University of Science and Technology), no. 1(27), pp. 15-21, 2023. ISSN 2225-9309 (Print).
Abstract: The article presents the algorithm for technological time series analysis and a heterogeneous model of anomaly detection detectors caused by an attacher attempting to intercept control or impose a control algorithm on a cyber-physical object. The proposed approach focuses on improving predictive analysis mechanisms as part of anomaly detection and elimination systems for production and process control systems of an ICS.

Key words: cyber-physical systems; anomaly detection system; data mining; neural networks; technological time series; autoencoders; long short-term memory.

About authors:

ATARSKAYA, Elena Andreevna, postgraduate student 1 year, Ufa state aviation technical University.

VULFIN, Alexey Mikhailovich, Associate Professor, Dept. of Computer Engineering and Information Security.

UZBEKOVA Liliya Yavgarovna, lecturer, Dept. of Computational Mathematics and Cybernetics