УДК 681.5.09:004.85

КЛАССИФИКАЦИЯ ОБОРУДОВАНИЯ ДЛЯ АВТОМАТИЗАЦИИ АНАЛИЗА ОТКАЗОВ СИСТЕМЫ КОНТРОЛЯ ОПАСНЫХ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ

Гребешков А.Ю., Кузнецов Я.М.

ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Самара, e-mail: grebeshkov-ay@psuti.ru

В настоящее время системы контроля опасных производственных объектов используются повсеместно. Предметом контроля является температура, влажность, энергопотребление, уровень загазованности, пожар, видеонаблюдение. Для контроля используются беспроводные сенсорные и мобильные сети. Последствия отказов оборудования контроля могут привести к потере данных и невозможности предотвратить ситуацию, потенциально опасную для жизни и здоровья людей. Для повышения надежности системы контроля опасных производственных объектов требуется автоматизация анализа сообщений об ошибках и отказах сенсорного и телекоммуникационного оборудования с помощью методов, основанных на знаниях. Это позволяет использовать различные источники данных о состоянии оборудования контроля в рамках единого семантического пространства описания этого оборудования. Создаётся интеллектуальная автоматизированная система, которая связывает данные о состоянии разнородных элементов системы контроля на основе понятий, которые этот элемент описывают, и связей между этими понятиями. Целью работы является повышение оперативности и надежности дистанционного контроля опасных производственных объектов, в том числе с использованием мобильных сетей путем классификации источников сообщений об отказах с помощью методов инженерии знаний и своевременного анализа состояния оборудования контроля с помощью машинного обучения. С помощью создаваемой семантической модели формируется классификатор оборудования управления. Классификатор оборудования управления используется далее как основа модели машинного обучения с учителем для автоматической классификации источников отказов и анализа сообщений об отказах классифицированного источника. Это позволяет автоматизировать управление системой контроля опасных производственных объектов.

Ключевые слова: анализ отказов, классификатор оборудования управления, система контроля опасного производственного объекта, семантическая модель, машинное обучение с учителем

EQUIPMENT CLASSIFY FOR FAILURE ANALYSIS AUTOMATION AT HAZARDOUS FACILITY CONTROL SYSTEM

Grebeshkov A.Yu., Kuznetsov Ya.M.

Povolzhskiy State University of Telecommunications and Informatics, Samara, e-mail: grebeshkov-ay@psuti.ru

These days hazardous facility control systems are used everywhere. The controlled parameters are temperature, humidity, energy consumption, carbon dioxide level, fire, video monitoring. Wireless sensor and mobile networks are used for hazardous facility control. Control equipment failures can lead to loss of data and make it impossible to prevent a potentially dangerous situation for ensuring the life and health of people. To improve the reliability of hazardous facility control systems, the automation of failure message analysis of sensor and telecommunication equipment with knowledge-based methods is required. This allows using heterogeneous data sources about the state of control equipment at a framework of single semantic space with description of this equipment. An intelligent automated system is created, which bind state data from different heterogeneous elements at the control system based on the object classes that describe these elements and the relations between these classes. The goal of the paper is to improve the efficiency and reliability of remote monitoring of hazardous industrial facilities, including the use of mobile networks, by classifying the sources of failure messages using knowledge engineering methods and timely analyzing of control equipment state using machine learning. With help of semantic model, a classifier of control equipment is formed. The control equipment classifier is used as the basis of a supervised machine-learning model for automatic classification of failure sources and analysis of failure messages at every classified source. This automating the management of hazardous facility control system.

Keywords: failure analysis, control equipment classifier, hazardous facility control system, semantic model, supervised machine learning

Для контроля состояния опасных производственных объектов (ОПО), определение которых дано в статье 2 Федерального закона от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов», часто применяют методы дистанционного контроля с помощью беспроводных сенсорных сетей [1, 2]. При эксплуатации ОПО могут возникнуть аварии или инциденты (аварийные ситуации), опасные для жизни и здоровья людей, выражающиеся в превышении норм температуры, влажности, загазованности, концентрации пыли, наличии пожара. Для своевременного выявления признаков опасной ситуации и принятия мер оперативного реагирования требуется обеспечить надежность и непрерывность мониторинга ОПО,

в том числе своевременно проводить идентификацию отказов оборудования системы контроля и выявление его аномального поведения. На практике сейчас это решается с помощью современных методов анализа и обработки информации. Поскольку вычислительные мощности отдельных сенсорных узлов ограничены, для обработки информации целесообразно использовать централизованные системы контроля с поддержкой методов и алгоритмов машинного обучения [3]. Имеется практический пример, где с помощью машинного обучения с учителем с достоверностью 91,62 % классифицирована ситуация деструктивного воздействия на датчики (сенсоры) [4]. Есть примеры идентификации аномального поведения сенсоров методом «случайного леса» с достоверностью от 94,4 до 97 % [5]. Однако в приведенных и аналогичных им случаях не рассматривались проблемы идентификации отказов и аномального поведения других компонентов системы дистанционного контроля ОПО, таких как шлюзы и транспортные сети. Поэтому требуется разработать комплексную систему классификации источников отказов, охватывающую все компоненты системы дистанционного контроля ОПО, включая шлюзы, транспортные сети, мобильные сети связи 4G/LTE. Функционально полная модель предметной области и связанный с ней классификатор оборудования позволят проводить комплексную обработку сообщений об отказах от разнородных, но при этом взаимосвязанных компонентов, своевременно фиксировать потерю данных мониторинга. Классификатор позволит выявлять ложные источники сообщений об отказах и достоверно определить класс (тип) отказавшего оборудования. Для классифицированных источников отказов далее методами машинного обучения определяются признаки отказа в виде увеличения доли ошибок или сбоев передачи, возникновения перемежающихся или полных отказов. В статье приводится пример программы машинного обучения и результат обработки сообщений о работе оборудования мобильной сети в составе системы дистанционного контроля ОПО. Реализация предлагаемого подхода позволит предотвратить потерю данных при управлении ОПО и своевременно отреагировать на аварийную ситуацию, что важно в связи с тем, например, что стоимость потерь в день из-за отказа только одного насоса на платформе нефтедобычи составляет до 300 тыс. долл. США, а использование предлагаемой модели, в том числе как элемента предиктивного управления, в той же нефтегазовой отрасли позволит снизить затраты на техническую эксплуатацию на 25–30 % [6].

Целью исследования является повышение оперативности и надежности дистанционного контроля опасных производственных объектов, в том числе с использованием мобильных сетей путем классификации источников сообщений об отказах с помощью методов инженерии знаний и своевременного анализа состояния оборудования контроля с помощью машинного обучения. Цель исследования достигается в случае корректной идентификации источника сообщений и последующего анализа сообщений об отказах с высокой достоверностью на выборке данных.

Материалы и методы исследования

Для описания знаний об оборудовании системы контроля опасных производственных объектов (СКОПО) использован онтологический подход [7], где указаны классы объектов и отношения между классами, причем классам присваиваются уникальные имена. Создаётся прикладная онтология предметной области с учетом результатов разработки онтологии предметной области Интернета вещей (IoT) [8, 9]. Материалы в виде непрерывной последовательности данных, совпадающих по месту, времени и способу измерения, получены для исследования от федерального оператора связи и сетей Интернета вещей, который повсеместно обеспечивает функционирование системы сбора информации о состоянии опасных производственных объектов в части энергопотребления, температуры, влажности, уровней загазованности, сигнализации систем пожарной безопасности. Собранные данные в СКОПО передаются через сети наземной подвижной радиотелефонной связи стандарта 4G/LTE. В целом система контроля опасных производственных объектов включает датчики, сенсорные узлы различных типов, шлюзы, которые далее используют сети 4G/LTE для дистанционного централизованного контроля, как показано на рис. 1. Эта схема далее является базовой для разработки классификации и применения метода машинного обучения с учителем.

Отказ сенсоров, шлюзов, компонентов сетей может являться причиной потери данных при сборе и передаче информации, в том числе когда используются технологии 4G/LTE [10]. Последовательность компонентов схемы на рис. 1 формирует «дерево отказов» СКОПО, причем отказ любого компонента схемы, от датчика до программного обеспечения СКОПО, приводит к потере данных и одновременно к прерыванию контроля параметров опасного производ-

ственного объекта [11]. Для своевременного выявления источника отказа или признаков предотказной ситуации СКОПО требуется представить совокупность знаний об оборудовании СКОПО в их взаимосвязи.

Пусть событие отказа семантически обозначается *Fault*. Тогда описать «отказ» как понятие в рамках СКОПО можно в виде кортежа:

$$Fault = \langle Cmpt, Attr(Cmpt), Rel(Cmtp) \rangle, \quad (1)$$

где *Fault* – общее обозначение отказа (или неисправности); *Cmtp* – компонент СКОПО, т.е. источник сообщений об отказах оборудования дистанционного контроля на рис. 1; *Attr(Cmpt)* – множество существенных свойств (атрибутов); *Rel (Cmpt)* – множество семантических отношений между компонентами СКОПО вида «относится к…», «влияет на…». Далее в рамках онтологического подхода разрабатывается классификация объектов предметной области. Классификация заключается в отнесении компонента – источника сообщений об отказе – к классу или фасете предметной области. Таким образом, проводится идентификация компонента, атрибутами которого *Attr(Cmpt)* являются типы сообщений. После этого проводится классификация сообщений идентифицированного объекта на сообщения о нормальной работе и на сообщения об отказах (ошибках). Также возможно разделение сообщений на штатные и распознаваемые и на аномальные и нераспознаваемые сообщения. Для этого используется контролируемое машинное обучение (Supervised Machine Learning, SML) или обучение с учителем, для чего строится дерево решений, причем в «узлах» дерева проводится проверка на соответствие классу значений атрибутов объекта [12]. В итоге происходит разбиение признаков компонентов (в данном случае – сообщений) на непересекающиеся области, а результатом становится класс или подкласс, к которому можно отнести сообщение классифицированного компонента. Также применяется алгоритм типа «случайный лес», который позволяет обрабатывать данные на большом количестве классов и атрибутов-признаков с возможностью обработки как вещественных, так и категориальных признаков [13]. В целом используемый онтологический подход и создаваемый классификатор позволяет формализовать знания экспертов предметной области, а появление аномальных результатов машинного обучения становится предлогом для изменения представления знаний о проблемной области.

Рис. 1. Схема организации системы дистанционного контроля опасного производственного объекта

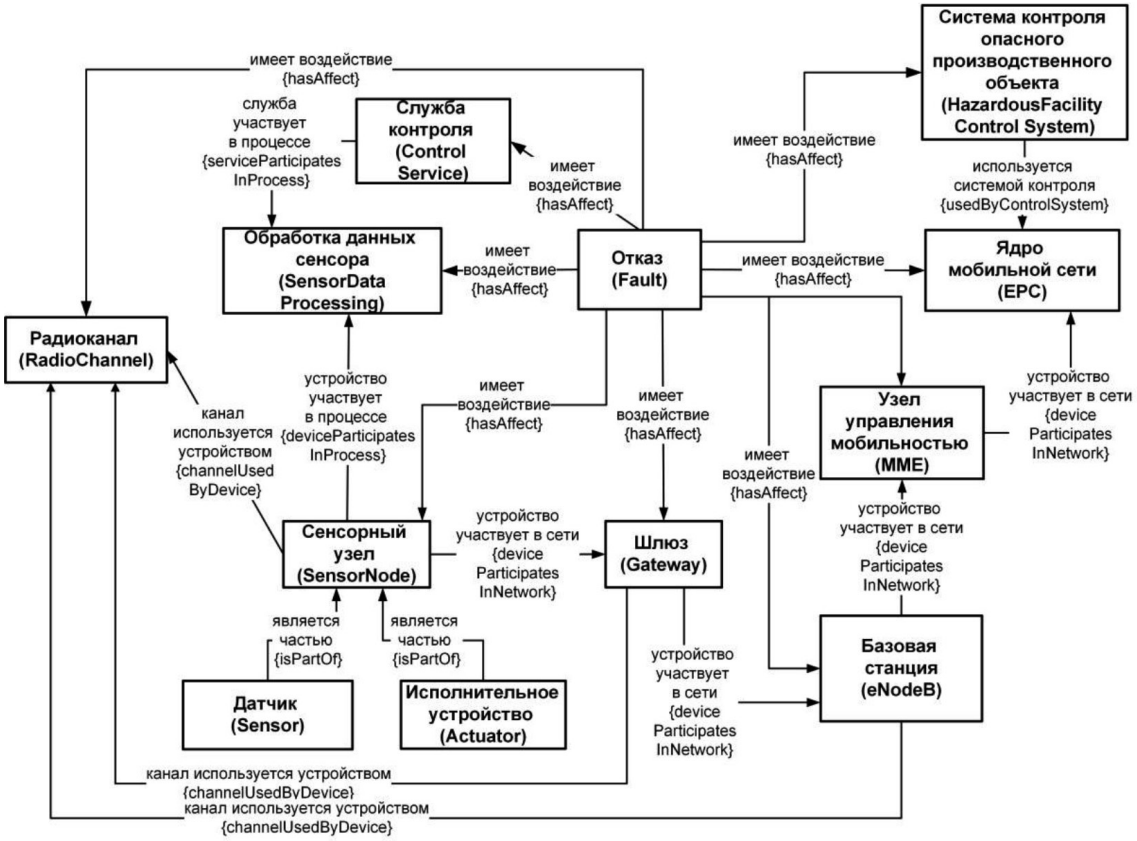

Рис. 2. Схема описания классов оборудования системы контроля опасного производственного объекта

Результаты исследования и их обсуждение

Для достижения цели исследования создаётся гибридный фасетный классификатор, где фасетный классификатор описан совокупностью классов, а свойства компонентов, отнесённых к определенному классу, рассматриваются как параметр фасеты и тоже могут быть классифицированы, например, по своему значению, если количество таких значений конечно. Для создания классификатора компонентов – источников отказов в рамках онтологического подхода экспертным путем разработан перечень взаимосвязанных классов физических или виртуальных компонентов системы контроля опасного производственного объекта согласно рис. 2. Здесь класс, как и все экземпляры, которые составляют каждый класс, связаны семантическими отношениями. Класс «Датчик» (Sensor) описывает множество устройств для измерения физических параметров окружающей среды. Класс «Исполнительное устройство» (Actuator) описывает множество устройств, способных наперед заданным способом изменять свои параметры в ответ на входной сигнал. Класс «Сенсорный узел» (SensorNode) описывает тип устройства, имеющего в своём составе датчик и, возможно, исполнительное устройство. Класс «Шлюз» (Gateway) описывает средство связи, соединяющее сенсорные узлы или отдельные сенсоры с другой сетью. Класс «Базовая станция» (eNodeB) описывает узел беспроводного доступа, на котором размещены функциональные элементы управления радиоресурсами, разуплотнения данных на линии передачи «во внешнюю сеть – вверх», средства шифрования пользовательских данных. Класс «Ядро мобильной сети» (EPC) описывает группу технических средств для усовершенствования систем мобильной связи или перехода с них на внешние системы.

Класс «Отказ» (Fault) описывает случайное событие нарушения работоспособного состояния оборудования или программного обеспечения. Класс «Радиоканал» (RadioChannel) описывает оборудование (антенны, излучатели, приемники), обеспечивающие обмен сигналом электросвязи в определенных полосах радиочастотного спектра. Класс «Узел управления мобиль-

ностью» (MME) описывает оборудование мобильной сети для управления режимом передачи, аутентификации и авторизации сенсорных узлов и шлюзов. Класс «Обработка данных сенсора» (Sensor Data Processing) предназначен для описания способа преобразования данных в ходе реакции чувствительного элемента сенсора на изменение окружающей среды. Класс «Служба контроля» (Control Service) описывает функциональные возможности системы контроля для оценки состояния производственного объекта по типу вещества реагирования (например, контроль влажности, загазованности, вибрации). Класс «Система контроля опасного производственного объекта» (Hazardous Facility Control System) описывает согласованное взаимодействия разных служб контроля и предоставление данных пользователям через человеко-машинный интерфейс. У рассмотренных классов и соответствующих экземпляров классов выделяются атрибуты. Атрибут есть описание свойства класса в форме свойства-литерала, если речь идёт об онтологии, или аналогично параметру фасеты, если речь идет о классификаторе. Типовым атрибутом является тип ошибки или отказа, установленного для каждого класса.

Формирование семантических отношений между классами также представлено на рис. 2. Отношение {*deviceParticipatesInNetwork*} указывает, что класс (и каждый экземпляр класса) «Сенсорный узел» участвует в сети, которая формируется классом «Шлюз». Аналогично класс «Шлюз» участвует в сети, создаваемой «Базовой станцией». Класс «Базовая станция» участвует в сети, формируемой «Узлом управления мобильностью». Отношение {*serviceParticipatesInProcess*} показывает, что класс «Служба контроля» связан с классом «Обработка данных сенсора» отношением, означающим, что служба участвует в процессе обработки сенсорных данных. Отношение {*systemParticipatesInProcess*} указывает на то, что класс «Система контроля производственного объекта» использует класс «Ядро мобильной сети» и таким образом связано с «Обработкой сенсорных данных» и со «Службой контроля». Отношение {*channelUsedByDevice*} показывает, что класс «Базовая станция» постоянно или временно использует класс «Радиоканал». Отношение {*usedByControlSystem*} показывает, что класс «Система контроля опасного производственного объекта» связан с классом «Ядро мобильной сети» и, следовательно, все отказы «Ядра мобильной сети» влияют на «Систему контроля опасного производственного объекта». Отношение {*hasAffect*} показывает, что класс «Отказ» связан со всеми классами, следовательно, каждый экземпляр каждого класса подвержен отказу. Как следует из приведенного описания, если два класса устройств связаны, к примеру, отношением вида {*deviceParticipatesInNetwork*} или {*systemParticipatesInProcess*}, то справедливы выражения вида

$$\forall Cmpt_i, Cmpt_j \quad deviceParticipatesInNetwork(Cmpt_i, Cmpt_j) \Rightarrow Fault(Cmpt_i) = Fault(Cmpt_j), \quad (2)$$

$$\forall Cmpt_i, Cmpt_j \quad deviceParticipatesInProcess(Cmpt_i, Cmpt_j) \Rightarrow Fault(Cmpt_i) = Fault(Cmpt_j), \quad (3)$$

где $Fault(Cmpt_i)$, $Fault(Cmpt_j)$ обозначают отказ i-го и j-го компонента соответственно.

Выражения (2) и (3) позволяют сделать вывод о том, что отказ одного из взаимосвязанных компонентов влияет и на другой компонент. Это ещё раз подтверждает необходимость наличия в модели классификатора для идентификации всех источников отказов в их взаимосвязи и взаимозависимости.

Поскольку ранее были приведены практические примеры классификации аномальных состояний для сенсоров, рассмотрим аналогичный подход в отношении оборудования мобильных сетей связи [14]. В работе [15] отмечалось, что качество соединений через сеть 4G/LTE определяется наличием или отсутствием ошибок протокола E-RRC (Evolved Radio Resource Control) и в особенности E-RAB (Evolved Radio Access Bearer) на экземплярах класса «Узел управления мобильностью». Поэтому выделение фасеты «Узел управления мобильностью» и классификация ошибок E-RAB, связанных с этим фасетом, можно признать существенной и рассматривать далее как источник данных для модельного анализа в рамках настоящей статьи.

Пусть классификатор с учетом выражений (1)–(3) выделил все сообщения протокола E-RAB для экземпляра класса «Узел управления мобильностью», причем среди этих сообщений есть сообщения о штатной работе и сообщения об отказе (нештатной работе), включая сообщения об 1, 2, 3 и 4 ошибках. Ошибки протокола E-RAB рассматриваются как причины потери данных СКОПО. Сообщения E-RAB разбиваются на обучающую (TrainData) и контроль-

ную выборки (TestTarget) из 36 890 наборов (строк) исходных данных. Пусть 80 % данных отнесены к обучающей выборке, которая используется для построения математических отношений между переменной цели «target» и предикторами, обозначенными как «train_cols». Контрольная выборка служит для получения классификации сообщений об ошибках протокола E-RAB на данных, которые не были использованы для обучения модели. Контрольная выборка составляет 20 % от объема исходных данных, т.е. показатель «test_size» = 0,2.

Для реализации классификатора используем среду программирования Python, где существует множество встроенных библиотек, в том числе для построения дерева решений (Decision Tree Classifier), что позволяет производить обучение модели на основе полученной обучающей выборки. Следует отметить, что в примере на рис. 3 значение «max_depth» задаёт максимальную глубину дерева решений, т.е. максимальное количество узлов, необходимых, чтобы достичь листа от корня, используя самый длинный путь, диапазон значений задается командой «range». В программном коде машинного обучения глубина «дерева» ограничена диапазоном от 1 до 9.

«Дерево» состоит из «узлов», и эти «узлы» выбираются таким образом, чтобы обеспечить оптимальное разделение функций. Для этого существуют разные критерии. В реализации дерева решений на языке программирования Python используются библиотеки программ с названием «scikit-learn», критерий задаётся параметром «criterion». Критерии «gini» и «entropy» используются для измерения качества разделения, причём «min_samples_split» – минимальное количество выборок, необходимое для разделения внутреннего «узла». Команда «GridSearchCV» реализует методы «соответствия» и «оценки», осуществляет исчерпывающий поиск по заданным значениям параметров для оценщика. Применение алгоритма производится последовательно на разделенных данных TrainData и далее испытывается на TestTarget. Команда model.score позволяет вывести на экран точность предсказания значений контрольной выборки.

Алгоритм «Случайный лес» на рис. 4 есть совокупность независимых деревьев решений, каждое из которых определяет принадлежность рассматриваемых объектов (сообщение протокола E-RAB) к определенному классу. Здесь максимальная глубина деревьев «случайного леса» (max_depth) задается равной 8, критерий разделения производится по энтропии (criterion = «entropy»), а параметр «max_features» ограничивает максимальное количество функций, которые следует учитывать при поиске разделения, параметр «n_estimators» определяет количество «деревьев», используемых в «лесу». Поскольку «Случайный лес» предусматривает создание нескольких деревьев решений, «n_estimators» используется для управления количеством деревьев. Далее «n_jobs» показывает количество задействованных ядер процессора для вычислений, при значении равном «-1» задействуются все ядра процессора.

Дерево решений.

```
model_DTC = DecisionTreeClassifier()
params_DTC = {'max_depth': range(1, 10),
              'criterion': ["gini", "entropy"],
              'min_samples_split': range(2, 10)}
cv = StratifiedKFold(shuffle=True, n_splits=5)
```

```
GS_DTC = GridSearchCV(estimator=model_DTC, param_grid=params_DTC, cv=cv, scoring="accuracy", n_jobs=-1)
```

```
model = DecisionTreeClassifier()
model.fit(X = TrainData, y = TrainTarget)
```

```
DecisionTreeClassifier(ccp_alpha=0.0, class_weight=None, criterion='gini',
                       max_depth=None, max_features=None, max_leaf_nodes=None,
                       min_impurity_decrease=0.0, min_impurity_split=None,
                       min_samples_leaf=1, min_samples_split=2,
                       min_weight_fraction_leaf=0.0, presort='deprecated',
                       random_state=None, splitter='best')
```

```
model.score(TestData,TestTarget)
```

Рис. 3. Последовательность программных команд для построения «Дерева решений»

Случайный лес.

```
model = RandomForestClassifier(criterion = 'entropy',
 max_depth = 8,
 max_features = 'log2',
 n_estimators = 7,
 n_jobs = -1)
model.fit(X = TrainData, y = TrainTarget)
```

```
RandomForestClassifier(bootstrap=True, ccp_alpha=0.0, class_weight=None,
                       criterion='entropy', max_depth=8, max_features='log2',
                       max_leaf_nodes=None, max_samples=None,
                       min_impurity_decrease=0.0, min_impurity_split=None,
                       min_samples_leaf=1, min_samples_split=2,
                       min_weight_fraction_leaf=0.0, n_estimators=7, n_jobs=-1,
                       oob_score=False, random_state=None, verbose=0,
                       warm_start=False)
```

```
model.score(TestData,TestTarget)
```

Рис. 4. Последовательность программных команд для построения «Случайного леса»

Результат работы алгоритма «Случайного леса» определяется путём голосования всех деревьев. Такой подход позволяет значительно повысить показатели качества анализа. В целом количество классифицированных обрывов соединений по причине ошибок протокола E-RAB на оборудовании MME в рамках контрольной выборки приведено на рис. 5.

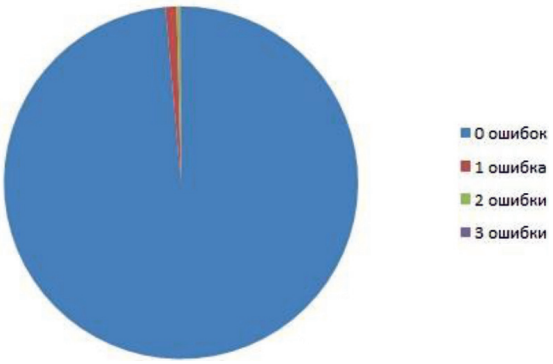

Рис. 5. Классификация сообщений протокола E-RAB при организации контроля опасного производственного объекта

Диаграмма на рисунке позволяет эксперту и (или) системе управления оценить стабильность и надежность системы контроля опасного производственного объекта с точки зрения классификации сообщений о работе протокола E-RAB. На рассматриваемом контрольном наборе данных часть сообщений о результатах работы протокола E-RAB, как атрибута классов объектов «MME», классифицирована как «0 ошибок». Точность построенного дерева решений для контрольной выборки равна 99,1% для метода дерева решений и 99,8% для алгоритма «случайного леса», т.е. наличие событий, классифицированных как 1, 2 или 3 ошибок протокола E-RAB, не превышает 0,9% в наихудшем случае. Таким образом, результат проведенных исследований свидетельствует об эффективности предлагаемой модели в целом, разработанного классификатора и применения метода машинного обучения с учителем для анализа функционирования сетей 4G/LTE в системах контроля опасных производственных объектов. Определено, что сеть 4G/LTE обеспечивает мобильность и надежность передачи данных дистанционного контроля, выраженных в высокой точности классификации состояний отказов на уровне 99,1%, что соответствует ранее приведенным данным для сенсорных сетей.

Заключение

Выполнен анализ предметной области классификации оборудования систем контроля опасных производственных объектов в части состава оборудования систем контроля и их возможных отказов. Классификация создаётся в рамках единого семантического пространства описания оборудования контроля, включая датчики, сенсоры, беспроводные сенсорные сети и сети мобильной связи. Выполнена разработка классов предметной области для представления знаний об источниках сообщений об отказах и взаимосвязи таких источников. Для автоматизации управления оборудованием системы контроля кроме классификатора предложе-

но использовать метод машинного обучения с учителем для отнесения поступающих сообщений от оборудования к данным об отказах или к данным о штатной работе. Рассмотрен практический пример применения классификатора и машинного обучения с учителем для сообщений от объекта классификации «Узел управления мобильностью». Показано, что в контрольной выборке данных классифицировано не более 1% сообщений об ошибках, что свидетельствует о надежности рассматриваемого узла MME с технологией 4G/LTE в части передачи данных мониторинга и допустимости его использования в системе контроля опасных производственных объектов.

Работа поддержана Фондом содействия инновациям (договор № 276ГУЦЭС8-D3/56326 от 26.12.2019 г.).

Список литературы

1. Тхань Фонг Ку Разработка и исследование беспроводной сенсорной сети для мониторинга угарного газа // Международный научно-исследовательский журнал. 2016. № 6–2. С. 148–153. DOI: 10.18454/IRJ.2016.48.171.

2. Барабанова Е.А., Мальцев Д.Б., Есауленко В.Н., Руденко М.Ф. Распределенная система контроля технологических объектов нефтегазовой промышленности на базе беспроводной сенсорной сети // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2017. № 2. С. 98–104. DOI: 10.24143/2072-9502-2017-2-98-104.

3. Erhan L., Ndubuaku M., Di Mauro M., Song W., Chen M., Fortino G., Bagdasar O., Liotta A. Smart anomaly detection in sensor systems: A multi-perspective review. Information Fusion. 2021. Vol. 67. P. 64–79. DOI: 10.1016/j.inffus.2020.10.00.

4. Pathak A.K., Saguna S., Mitra K., Åhlund C. Anomaly detection using machine learning to discover sensor tampering in IoT systems // Proceedings of IEEE International Conference on Communications (ICC 2021, Dublin, Ireland, 14–23 June 2021). IEEE, 2021. P. 1–6. DOI: 10.1109/ICC42927.2021.9500825.

5. Haji S.H., Ameen A.Y. Attack, and anomaly detection in IoT networks using Machine Learning techniques: A Review. Asian journal of research in computer science. 2021. Vol. 9 (2). P. 30–46. DOI: 10.9734/AJRCOS/2021/v9i230218.

6. Stevenson W.D. The Future is Smart. HarperCollins Leadership, 2018. 256 p.

7. Горшков С.В., Гумеров С.З., Кралин С.С., Мирошниченко М.Г., Муштак О.И., Шебалов, Р.Ю. Онтологическое моделирование предприятий: методы и технологии; отв. ред. С.Е. Горшков. Екатеринбург: Изд-во Уральского ун-та, 2019. 236 с.

8. Song Z., Cardenas A.A., Masuoka R. Semantic middleware for the Internet of Things. Proceedings of 2nd International Internet of Things Conference (IoT, Tokyo, Japan, November 30 – 1 December 2010). IEEE, 2010. P. 1–8. DOI: 10.1109/IOT.2010.5678448.

9. Tao M., Ota K., Dong M. Ontology-based data semantic management and application in IoT-and cloud-enabled smart homes. Future Generation Computer Systems. 2016. Vol. 76. 22 P. DOI: 10.1016/j.future.2016.11.012.

10. Kreher R., Gaenger K. LTE signaling, troubleshooting and performance measurement. Wiley, 2016. 368 p.

11. Гребешков А.Ю., Кузнецов Я.М. Машинное обучение при прогнозе неисправностей беспроводных сетей // Сборник материалов XXVII Российской научной конференции профессорско-преподавательского состава, научных сотрудников и аспирантов ПГУТИ (Самара, 27–31 января 2020 г.). Самара: ПГУТИ, 2020. С. 26–27.

12. Некрасов И.В., Правдивец Н.А. Машинное обучение в задачах прогноза отказов оборудования // 19-я Всероссийская конференция с международным участием «Математические методы распознавания образов» (ММРО–2019)»: тез. докл. (Москва, 26–29 ноября 2019 г.). М.: ИСП РАН, 2019. С. 371.

13. Чио К., Фримэн Д. Машинное обучение и безопасность. М.: ДМК Пресс, 2020. 388 с.

14. Morocho-Cayamcela M.E., Lee H., Lim W. Machine learning for 5G/B5G mobile and wireless communications: potential, limitations, and future directions. IEEE Access. 2019. Vol. 7. P. 137184–137206. DOI: 10.1109/ACCESS.2019.2942390.

15. Фадеев В.А., Корсукова К.А., Надеев А.Ф. Анализ обрыва соединений по протоколу E-RAB мобильной сети LTE/LTE-A // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 12. С. 4–12. DOI: 10.24411/2072-8735-2018-10327.