УДК 656.628

Модель идентификации технического состояния устройств информационно-телекоммуникационных сетей подсистемой сетевого мониторинга

Аллакин В. В.

Постановка задачи: *обосновать моделирование идентификации основных видов технического состояния устройств информационно-телекоммуникационных сетей общего пользования на основе методов системного анализа и многоуровневого подхода к описанию сложных технических систем.* ***Цель работы:*** *разработать модель идентификации технического состояния устройств информационно-телекоммуникационных сетей подсистемой сетевого мониторинга в интересах повышения эффективности ее функционирования на различных логических уровнях.* ***Используемые методы:*** *модели многоагентных (мультиагентных) систем интеллектуальной поддержки принятия решения, методы многоуровневого синтеза сложных технических систем, методы теории надежности (функциональный контроль, мониторинг, контроллинг), методы теории классификации, методы идентификации вида состояния технического устройства на основе критерия Неймана-Пирсона, методы теории графов.* ***Новизна*** *исследования состоит в том, что предложенная модель идентификации технического состояния сетевого устройства подсистемой мониторинга в отличие от известных имеет иерархическую структуру, на основании чего позволяет осуществлять перераспределение функций центра управления сетью и периферии в зависимости от текущего состояния системы с использованием агентно-ориентированного подхода. При этом обоснованы и описаны аналитически шесть классов технического состояния сетевого устройства с учётом ошибок контроля первого и второго рода.* ***Результат*** *проведенного исследования состоит в получении математических выражений для оценки вероятности работоспособного состояния и вероятности отказа сетевого устройства в процессе многоэтапного принятия решения с задействованием не только сервера мониторинга на локальном уровне иерархии сети, но и подсистемы мониторинга более высокого (регионального) логического уровня и всей информационно-телекоммуникационной системы в целом. Используемый при моделировании многоуровневый подход позволяет осуществлять более точную идентификацию функционального состояния сетевого элемента, когда на первом этапе по локальной информации, содержащейся в сервере мониторинга, определяется наличие нарушения режима работы, а на втором и последующих этапах уточняется степень и тип нарушения. Каждый этап связан с соответствующим уровнем иерархии. При выявлении аномальных ситуаций осуществляется рассылка интеллектуальных агентов, пронумерованных по уровням иерархии, которые управляют состояниями сетевых устройств, приводя их в нормальное состояние.*

Ключевые слова: *информационно-телекоммуникационная сеть, подсистема мониторинга, логический уровень, ошибки первого и второго рода, сервер мониторинга, идентификация.*

Актуальность

На сегодня стремительное развитие информационных технологий (IT) привело к постоянному совершенствованию и эволюционированию современ-

Библиографическая ссылка на статью:
Аллакин В. В. Модель идентификации технического состояния устройств информационно-телекоммуникационных сетей общего пользования подсистемой сетевого мониторинга // Системы управления, связи и безопасности. 2021. № 5. С. 40-64. DOI: 10.24412/2410-9916-2021-5-40-64

Reference for citation:
Allakin V. V. A model for identifying the technical condition of information and telecommunication network devices by a network monitoring subsystem. *Systems of Control, Communication and Security*, 2021, no. 5, pp. 40-64 (in Russian). DOI: 10.24412/2410-9916-2021-5-40-64

ных информационно-телекоммуникационных систем и сетей (ИТКС) как общего пользования (ОП) так и специального назначения [1, 2], которые строятся на основе многоуровневой модели взаимодействия открытых систем (ЭМВОС) OSI, цифровых сетей с интеграцией служб (ISDN) и сетей связи следующего поколения (NGN). При этом их техническая платформа представляется структурированной совокупностью скоростных каналов связи, узлов коммутации, серверов услуг и сервисов связи, действующих в интересах пользователей сети, а также иерархической автоматизированной системы управления связью (АСУС), фундаментальным требованием которой на гетерогенной ИТКС является эффективный *мониторинг* ее ресурсов [1] для точного и актуального обновления в интересах поддержки своевременной реконфигурации сети с целью устранения предотказного ее состояния и недопущения аварии.

Согласно [3] под *мониторингом* технического состояния (ТС) понимается составная часть технического обслуживания, заключающаяся в наблюдении за объектом с целью получения информации о его ТС и рабочих параметрах. Термин «техническое состояние» как совокупность свойств объекта контроля (ОК) существенно отличается от обычного понятия «состояние» любого функционирующего объекта, обозначающего совокупность значений внутренних параметров в каждый момент времени, которые имеют место в результате целенаправленного управления ими в ходе использования объекта по назначению. Поэтому в работе термин «состояние» используется соотносительно к ИТКС, а термин «техническое состояние» соотносительно к сетевым устройствам.

Базовые понятия надежности, работоспособности и поддержки функциональной устойчивости сетевых структур определены в международном стандарте ISO 9126:1991 [4], предусматривающем два основных направления поддержки функциональной безопасности: обеспечение надежности функционирования и ее оценку. Обычно модели оценки основаны на математическом аппарате теории надежности с принятыми допущениями и ограничениями, влияющими на оценку. При этом в качестве основных источников информации принято считать процессы тестирования ИТКС в различных условиях внутренних и внешних воздействий.

Классификационно различают аналитические и эмпирические модели оценки надежности, функциональной устойчивости и работоспособности ИТКС. Причем если аналитические модели позволяют вычислить количественные показатели надежности системы, используя данные о ее поведении в процессе тестирования, то эмпирические – в основном базируются на анализе особенностей ее структуры. В свою очередь в классе аналитических моделей рассматриваются динамические модели, в которых проявление отказов системы наблюдают во времени, и в статике, когда число отказов зависит от числа прогонов теста или от характеристик входных данных.

При проектировании сложных технических систем, таких как ИТКС, для определения отказов обычно используются структурные схемы надежности, в которых элементы системы соединяются между собой различными способами: последовательно, параллельно, смешанно или произвольно [5]. В таких структурных схемах надежности в качестве основных показателей оценивают веро-

ятность безотказной работы и вероятность отказа. Причем здесь в качестве основных динамических аналитических моделей используют модели Шумана, Ла Падула, Муса, Джелинского-Моранды, Шика-Вольвертона, переходных вероятностей, а в качестве основных статистических аналитических моделей – модель последовательностей испытания Бернулли, модели Нельсона, Липова, Милса. Данные модели представляют подход, имеющий ограничение в виду с ведением постоянного тестирования современных сетевых инфраструктур. При этом в случае отсутствия информации наблюдения за сетевым элементом ИТКС или прекращения ее обновления на рабочем месте администратора подсистемы мониторинга в процессе тестирования рассматривается как отказ системы. Действительно, для поддержания функциональной безопасности устройств и узлов распределенной инфраструктуры современных ИТКС, протекающие в них процессы должны подвергаться постоянному контролю и мониторингу [6].

Оценка изменений температуры, электромагнитных и звуковых спектров, амплитуды и частоты вибраций и т. д., получаемая от сенсоров и датчиков при тестировании и функционировании сетевых элементов во времени может заблаговременно сигнализировать о нарастании в них предаварийных процессов, ведущих к аномальному состоянию, аварии или отказу. Поэтому альтернативой различных видов аналитических моделей могут служить прогнозные модели, на основе оценок технических характеристик объекта мониторинга: выход параметра за пределы допуска, структура, число отказов и пр.

Мониторинг в информационно-телекоммуникационной (IT) отрасли, будь то небольшая компания или огромный центр обработки данных (ЦОД), необходим для того, чтобы системные администраторы ИТКС были оповещены раньше или хотя бы одновременно с пользователями об отказах и проблемах в сетевой инфраструктуре. Необходимость прогноза, а тем самым и предотвращение отказов, своевременное оповещение о них оператора и хранение информации о техническом состоянии ИТКС и элементов сети обеспечивает *актуальность* данной работы.

В современных системах мониторинга динамика объекта управления (сетевого элемента, канала, сети) представляется как последовательность переходов между стационарными состояниями. Примеры данного утверждения приведены в ГОСТ 27.002-2015 [3], где рассмотрены виды состояния технических объектов (ОК): исправное, неисправное, работоспособное (рабочее), неработоспособное (нерабочее), предельное, опасное, предотказное. Однако, предотказное состояние сетевого элемента предполагает диапазон отклонений (изменяемости) контролируемых параметров от нормы, поскольку «… характеризуется повышенным риском отказа ОК». Данное утверждение не противоречит Рекомендации М.3703 Международного Союза электросвязи [7].

Важно отметить, что работоспособное состояние разных сетевых устройств, размещаемых на различных логических уровнях сети и в условиях функционирования при различной нагрузке имеют разную вероятность перехода из одного в другой вид состояния – предотказное или неработоспособное, а также имеют различную тенденцию развития отказа. Поэтому и методы иден-

тификации видов состояний для сетевых устройств, либо отдельных сегментов сети, либо всей сети на более высоком уровне обобщения должны отличаться. Для чего необходимо осуществить *моделирование* процесса идентификации основных видов ТС, а также оценку вероятности его отсутствия (нормального функционирования). Далее рассмотрим вопросы моделирования видов ТС ИТКС на её логических уровнях. При этом на нижнем (локальном уровне) речь будет идти о техническом состоянии сетевого устройства, а на глобальном и региональном уровнях – о состоянии сети и ее сегмента в целом.

Цель статьи: моделирование процесса идентификации основных видов технического состояния (работоспособного, неработоспособного и предотказного) элементов и узлов ИТКС ОП.

Место мониторинга в общей процедуре контроля и диагностики

Развитие научных представлений о *мониторинге*, как разновидности процедуры контроля, существенно зависит от методологической разработки контроля и, прежде всего, от состояния терминологии. Термин «контроль» происходит от французского слова *contrerole* – список, ведущийся в двух экземплярах. Первоначально он означал проверку документации, а затем проверку объектов различной природы. В этой трактовке он вошел в русский язык и употреблялся как синоним термина «проверка», как совокупность действий, устанавливающая правильность или ошибочность чего-либо [8]. В этом случае контроль сводится к установлению принадлежности конкретной ситуации случайной величины или функции, отображающих свойства ОК, норме. Для технических объектов согласно [9] различают такие *виды контроля* как: контроль готовности, контроль функционирования и контроль поисковый.

Для эффективной эксплуатации сетевого оборудования современных ИТКС необходимо знание соответствия значений параметров ОК требуемым, а также его вида ТС в реальном масштабе времени, или близкому к нему. С данной точки зрения, важно иметь оценки результатов *контроля функционального* в масштабе *реального времени*, с целью недопущения развития предотказного ТС в аварию и своевременного обнаружения факта изменения вида ТС ОК. Особенно это критично для сетевого оборудования, функционирующего в автоматическом режиме в филиалах основных офисов компаний, на значительных удалениях от диспетчерского пункта управления (ДПУ) без постоянного присутствия инженерно-технического персонала, способного вовремя предотвратить отказ. Это возможно только проведением непрерывного либо периодического функционального контроля, что можно рассматривать по определению, соответственно, как *мониторинг* или *контроллинг* [3, 10].

В то же время проведение метрологических мероприятий полного (инструментального) контроля всех параметров изделия в соответствии с нормативно-технической документацией (НТД) либо сокращенного контроля ограниченного числа его параметров предусмотрено исключительно при проведении процедур *контроля готовности*, в ходе технического обслуживания (ТО). В процессе же *контроля функционирования* ОК проведение постоянного мониторинга и периодического контроллинга *всех* эксплуатационных параметров не-

приемлемо с экономической точки зрения, низкой оперативности цикла проведения полного контроля, а также использования результатов такого контроля на фоне скоротечности развития аварийной ситуации (отказа) [11].

Традиционная модель контроля ТС сетевого оборудования весьма уязвима для критики. Действительно, «узость» модели, «жесткость» ее исходных предпосылок проявляются в следующем:

1. Говоря о том, что средство мониторинга «осуществляет сбор» контролируемых метрик параметров, мы игнорируем тот факт, что в действительности средство взаимодействует не с отдельным параметром (физической величиной), а с некоторым реальным исследуемым объектом. Мониторинг должен рассматриваться как познавательный процесс, в результате которого можно получить *многомерное* описание всего исследуемого ОК в количественных терминах, как модель объекта или связанные с ней отдельные характеристические свойства объекта. Только числовые значения физических величин без указания их связи с моделью объекта не позволяют использовать или интерпретировать результат мониторинга с высокой достоверностью.
2. Моделирование самого процесса мониторинга должно охватывать наряду с вопросом разработки алгоритма, который бы реализовал модель проверки принадлежности контролируемого параметра (его метрики) к норме, так же непосредственно обоснование выбора такой нормы. Данный вопрос должен решаться как с учетом целей мониторинга, так и условий функционирования ОК (режимов работы, условий эксплуатации, нагрузки и пр.). Желательно при этом использовать такой способ выражения нормы в виде эксплуатационного допуска на метрику параметра, при котором ее значение характеризует степень достижения ОК поставленной цели. Таким образом, одному и тому же исследуемому объекту мониторинга ставится в соответствие та или иная модель, исходя из условий применения по назначению и необходимого качества функционирования, т. е. актуально применение *профилактических допусков*, вводимых для разных режимов и условий эксплуатации [12].
3. При этом совершенно очевидно, что двухинтервальное решение «годен-негоден» по результатам процедуры (цикла) мониторинга является недостаточным. В большинстве случаев подсистема мониторинга должна иметь информацию об остаточном ресурсе ОК, т. е. о том насколько близко его ТС к аварийному. Как правило, аварийному режиму функционирования ОК предшествует предотказное ТС, имеющее некоторый временной интервал и характеризуемое повышенным риском возникновения отказа (аварии). Действительно, с точки зрения функциональной надежности каждого эксплуатанта и телекомоператора в большей степени интересует переход из работоспособного в неработоспособное ТС через промежуточное – предотказное ТС. Учитывая это, разбиение, которое должно соответствовать предотказному ТС, может уточняться для каждого ОК или его измеряемого параметра. При этом задачей подсистемы мониторинга является своевре-

менное обнаружение предотказного ТС сетевого устройства с целью оперативного (превентивного) принятия мер для недопущения развития отказа (аварии).

4. Очевидно также, что в результате мониторинга должна быть получена информация о наблюдаемом сетевом устройстве, необходимая для управления им или системой, состоящей из этих устройств, т. е. мониторинг не является целью, а лишь средством для ее достижения. В связи с чем задача создания моделей, методов и средств мониторинга должна рассматриваться в непосредственной связке с вопросом об использовании его результатов и как одна из сторон более общей задачи – управления реальными объектами. Основной задачей системы мониторинга является получение информации для выработки необходимых управляющих воздействий на ОК и систему эксплуатации с целью обеспечения максимального эффекта от использования объекта мониторинга по назначению.
5. Кроме того, в традиционной модели не находит отражения связь объекта и системы мониторинга с внешней средой, с фактами, не связанными с исследуемым объектом, но оказывающими влияние на результат мониторинга. Такие факты многочисленны и многообразны: произвольные сочетания внешних условий, в которых функционирует объект или производится измерительный эксперимент, нестабильность характеристик системы мониторинга и неидеальность образцовой меры и другие факторы, в совокупности называемые *внешними факторами*. Необходимость их учета следует также из представленного в [3] определения ТС как «состояния, которое характеризуется в определенный момент времени, *при определенных условиях внешней среды*, значениями параметров, установленных технической документацией на объект».
6. Процессы мониторинга ТС на территориально-распределенных ИТКС в настоящее время пока еще не соответствуют современному уровню автоматизации технических систем, например, в различных областях промышленности (таких как развитие SCADA-системы, IoT и др.), поскольку классический подход к развитию систем мониторинга «вытекает» из эволюционирования систем контроля, не обеспечивающих достаточно быструю (в режиме on-line) реакцию на запросы специалистов, несмотря на бурное развитие современных средств связи и IT отрасли в целом.
7. Современные ИТКС строятся на основе многоуровневой модели ЭМВОС (OSI), в то время как классический подход к контролю работоспособности, базирующийся на метрологии как науке об измерении физических параметров, ориентирован, в основном, на задачи первого уровня модели. В то же время появление новых технологий беспроводного доступа, информационной поддержки жизненного цикла (ЖЦ) (CALS-технологии), технологий искусственного интеллекта (извлечения знаний из различных стационарных и мобильных источников, прогнозирования и поддержки принятия решений в режиме on-line, когни-

тивного анализа данных, мультиагентного управления и диспетчеризации ресурсов в распределенных мобильных системах и др.), показывают направление развития данной предметной области и на других уровнях OSI.

Исходя из этого, необходим поиск новых подходов к моделированию процесса мониторинга функционального состояния сетевых устройств, сегментов сети и ИТКС в целом, удовлетворяющего всевозрастающим требованиям по оперативности мероприятий поддержания готовности элементов сети к применению по назначению в различных внешних и внутренних условиях функционирования. Они должны отличаться наглядностью и простотой с точки зрения удобства применения SLA-инженером подсистемы мониторинга ИТКС или лица, принимающего решение (ЛПР) на переконфигурацию сети.

Многоуровневый и мультиагентный подходы к моделированию структур ИТКС ОП и ее подсистемы мониторинга

Подходя к вопросу моделирования оптимальных систем контроля и диагностики необходимо отметить, что данным направлением занимались научные школы таких ученых как: Н. П. Байда, А. К. Дмитриева, А. Г. Дмитриенко, Г. Д. Петрова, А. И. Птушкина, Р. М. Юсупова и др. Общим методам управления (контроля) распределенными системами посвящены работы В. С. Анфилатова, Н. П. Бусленко, С. Н. Бушуева, Я. С. Дымарского, Л. Лэсдона, М. Месаровича, Д. Мако, Н. Н. Моисеева, А. А. Привалова, Я. Такахара, Д. Б. Юдина и др. Методам идентификации характеристик случайных процессов посвящены работы Н. К. Кульмана, Дж. Мелса, Б. Т. Поляка, В. С. Пугачева, И. Н. Синицына, Ю. Г. Сосулина, Р. Л. Стратоновича, Э. П. Сэйджа, В. И. Тихонова, К. Фокунага, Я. З. Цыпкина и др. Для проведения автоматических (автоматизированных) дистанционных измерений, передачи измерительной информации (ИИ) о ТС ОК применяют информационно-измерительные (ИИС) и телеметрические системы (ТМС), значительный вклад в теорию и практику создания которых внесли отечественные и зарубежные ученые: Д. Бэйли, В. А. Ильин, Е. Е. Исаков, В. А. Ловцов, А. В. Назаров, Г. Г. Раннев, А. В. Фремке, Е. Н. Хохлачев, Т. Хаусли и др.

При этом важно отметить, что моделирование систем контроля и мониторинга невозможно без использования многоуровневого подхода к синтезу ИТКС ОП, чему посвящено большое количество публикаций отечественных и зарубежных специалистов в области автоматизированных (автоматических) систем контроля ТС. Среди них особого внимания заслуживают монографии и труды Л.Г. Евланова, А. В. Кучерявого, А. М. Лихачева, В. Н. Посупонько, В.В. Федоренко, Е. А. Чернявского и др.

Эффективность обеспечения нормального функционирования ИТКС ОП во многом зависит от реализации комплексного использования перечисленных выше подходов к построению сетевой инфраструктуры на основе соответствующего моделирования видов ТС ее функциональных элементов, методов мониторинга и управления на сети и др. Поскольку известно, что современные ИТКС работают на глобальном, региональном и локальном уровнях, для моде-

№5. 2021
ISSN 2410-9916

лирования её подсистем и информационных трактов (ИТ) передачи телеметрической информации (ТМИ) используем многоуровневый подход [13] к построению подсистемы мониторинга состояния элементов на территориально-распределенной системе.

Так на рис. 1 приведена логическая схема функционирования ИТКС в виде ИТ доступа из локальной вычислительной сети (локальный уровень – ЛВС) к глобальной компьютерной сети (ГКС) (глобальный уровень – ГКС «Интернет»).

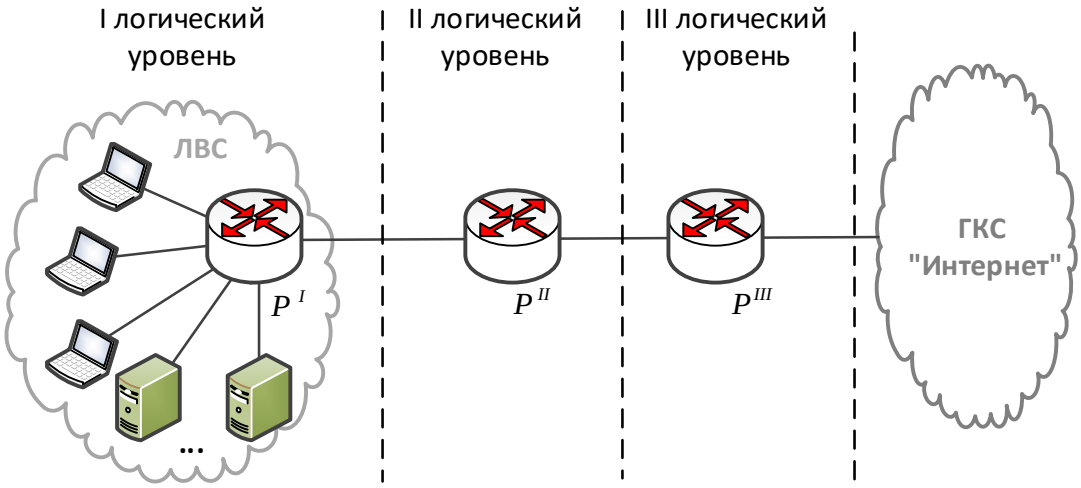

Рис. 1. Логическая схема функционирования информационного тракта ИТКС

На представленной схеме показано, что доступ к тому или иному узлу (сетевому устройству) ИТКС осуществляется по ИТ передачи сигналов телеизмерения (ТИ) и телесигнализации (ТС), через соседние её узлы (сетевые устройства), имеющие связность с ним и расположенные на сопрягаемых логических уровнях («локальный-региональный», «региональный-глобальный»). При этом на рисунке показаны: I – логический уровень, на котором обеспечивается доступ подсистемы мониторинга в ИТКС (к её сетевым устройствам) при решении прикладных задач; II – логический уровень, занимающий промежуточное звено между ЛВС и ГКС, решающий задачи коммутации и маршрутизации; III – логический уровень сопряжения с ГКС [14].

Важно отметить, что работоспособное состояние разных сетевых устройств на различных логических уровнях и при различной нагрузке (сетевого трафика) имеют разную вероятность перехода из работоспособного состояния в предотказное или неработоспособное (аварийное) и наоборот, а также имеют различную тенденцию развития отказа (аварийной ситуации). Поэтому и методы выявления (идентификации) видов состояний для сетевых устройств, либо сегментов сети на более высоком уровне обобщения должны отличаться. Для чего необходимо осуществить моделирование наступления основных видов состояний функциональной безопасности, а также оценку вероятности его отсутствия (нормального функционирования системы).

Модель подсистемы мониторинга ИТКС ОП предлагается строить по нескольким контурам управления в зависимости от размещения сетевого устрой-

DOI: 10.24412/2410-9916-2021-5-40-64
URL: https://sccs.intelgr.com/archive/2021-05/03-Allakin.pdf

ства относительно наблюдаемого его сервера мониторинга. При этом ИТКС, как сложную территориально-распределенную систему, совмещающую в себе $N(k)$ подсистем (подсетей) и сетевых устройств на каждом из k-м уровне управления (локальном, региональном, глобальном), в условиях воздействия на них внутренних и внешних дестабилизирующих факторов (ДФ), контролируют на K уровнях, где $K \geq 3$, $k = 1, 2,\ldots, K$. Причем каждый $n(k)$-й узел характеризуют $M(k, n)$ контролируемыми параметрами (метриками), на которые заблаговременно должны быть установлены пороговые значения $z^{\text{пор}}(k, n, m)$, где $n(k) = 1, 2,\ldots, N(k)$, $m = 1, 2,\ldots, M(k, n)$.

В ходе выполнения процедуры мониторинга ИТКС серверы мониторинга, наблюдающие сетевые устройства, осуществляют сбор измерительной информации (метрик) $z(k, n, m)$ их параметров на каждом уровне для сравнения с заданными предварительно пороговыми значениями $z^{\text{пор}}(k, n, m)$. При этом оценку состояния всей ИТКС проводят последовательно по K этапам. Сначала происходит сравнение измеренных значений параметров сетевых устройств первого (локального) логического уровня ИТКС с пороговыми значениями. Если измеренные значения находятся в пределах допусков, то ее считают работоспособной. При выходе параметров за пределы пороговых значений происходит генерация управляющего интеллектуального агента (ИА) для последовательной оценки состояния ИТКС, принадлежащих ее вышестоящим логическим уровням управления. Для этого сравниваются измеренные и пороговые значения параметров узлов системы k-го уровня. При этом, в случае если измеренные значения находятся в пределах заданных, то подсистему на k-м логическом уровне ИТКС считают работоспособной, иначе происходит идентификация неработоспособного состояния подсистемы с указанием её параметров, которые вышли за пределы пороговых значений. В соответствии с результатом контроля происходит генерация интеллектуально агента с управляющим воздействием на их резервирование и в последующем – на восстановление. Важно отметить, что допустимые пороговые значения параметров (метрик) сетевых устройств задаются исходя из априорных данных о текущем состоянии ИТКС на каждом из логических уровней, формируя при этом контур обратной связи.

При построении сложных технических систем, к которым можно всецело отнести ИТКС, зачастую пользуются моделями многоагентных (мультиагентных) систем (МАС) интеллектуальной поддержки принятия решения с синергетической оценкой, учитывающей целостность комплекса показателей (параметров, как всей системы, так и её подсистем) [15]. Мультиагентные системы, построенные на базе использовании методов распределенного искусственного интеллекта (РИИ) работают на применении правил и рассуждений, основанных на прецедентах. В них каждый интеллектуальный агент рассматривается как система, основанная на знаниях, с применением компонентов, которые обеспечивают безопасность, надежность функционирования, качество обслуживания, взаимодействие с другими агентами и сетевыми ресурсами. Фактически такая организация МАС реализует информационную архитектуру функциональной модели FCAPS [16], включающую пять основных «функциональных проекций» систем управления и систем мониторинга (управление отказами (Faults); управ-

ление конфигурацией (Configuration); управление производительностью (Performance); управление ресурсами (Accounting); управление безопасностью (Security), таблица 1) и обладает преимуществами в виде удобств использования методов представления знаний, разработанных в рамках искусственного интеллекта [15].

Таблица 1 – Задачи мониторинга согласно модели FCAPS

(F) Мониторинг отказов	(C) Мониторинг конфигурации	(A) Мониторинг производительности	(P) Мониторинг ресурсов	(S) Мониторинг безопасности
Обнаружение отказов	Раскрытие топологии и конфигурации сети	Мониторинг степени загрузки и степени доступности (availability)	Мониторинг использования ресурсов	Сбор и агрегация журналов доступа к ресурсам
Корреляция отказов (выявление отказа – первопричины в группе отказов)	Мониторинг топологии и конфигурации сети	Сбор данных о производительности сети	Установка порогов использования ресурсов	Предупреждение о проблемах безопасности/ отчетов безопасности
Генерация предупреждений		Создание отчетов о производительности	Аудит журналов доступа к ресурсам	Мониторинг и проверка прав доступа пользователей
Обработка предупреждений		Анализ данных о производительности	Отчетность об использовании	Мониторинг попыток нарушения безопасности
Фильтрация предупреждений		Отчетность об ошибках		Анализ журналов доступа к ресурсам
Диагностическое тестирование		Сбор статистики о производительности		
Журнализация ошибок		Ретроспективный анализ данных и прогнозирование		
Обработка ошибок				
Статистика ошибок				

МАС включают в себя широкий круг наукоемких информационных технологий, в основе реализации которых находятся научно-методический аппарат распределенной обработки данных и РИИ. Выработка самостоятельного направления исследований в РИИ со своим предметом и объектом исследования основана на допущении, что каждый элемент сети в виде ИА (решатель) может автономно решать достаточно сложные задачи, но при этом общая задача подсистемы мониторинга не может быть решена без сотрудничества сетевых устройств, поскольку никакое отдельное сетевое устройство не обладает информацией, знаниями, а также вычислительными ресурсами, необходимыми и достаточными для ее решения.

При формировании теоретических основ построения МАС выделяют микротеорию, которая включает вопросы построения отдельно взятого ИА, и макротеорию, рассматривающую направления взаимодействия ИА в МАС. Согласно первой теории, интеллектуальный агент рассматривается как система, обладающая свойствами автономности, активности, реактивности и социальности. Согласно второй теории – ИА это интенсиональная система, при специфицировании которой используются такие категории как знания, намерения, убеждения, обязательства, желания и пр. [15].

Учитывая данные подходы, моделирование процедуры идентификации ТС элементов территориально распределенной ИТКС может быть реализовано на основе МАС, представляющей собой совокупность ИА, размещаемые на сетевых устройствах и серверах мониторинга, и включающей в себя уровни реактивного поведения, оценки состояния ОК, прогноза и планирования как автономных, так и совместных действий на сети. Целенаправленное реактивное поведение ИА в аварийных ситуациях, при воздействии ДФ на сетевое устройство (сегмент сети), обычно требуют планирования последовательности шагов, которые направлены на достижение требуемого ТС сетевого устройства (работоспособного состояния). Причем в каждой ситуации существует несколько возможных планов действий. Поэтому ИА должен оценить и сравнить эффективность доступных планов действий с учетом их полезности. В такой интерпретации функций ИА, учитывающего полезность действий представлена на рис. 2.

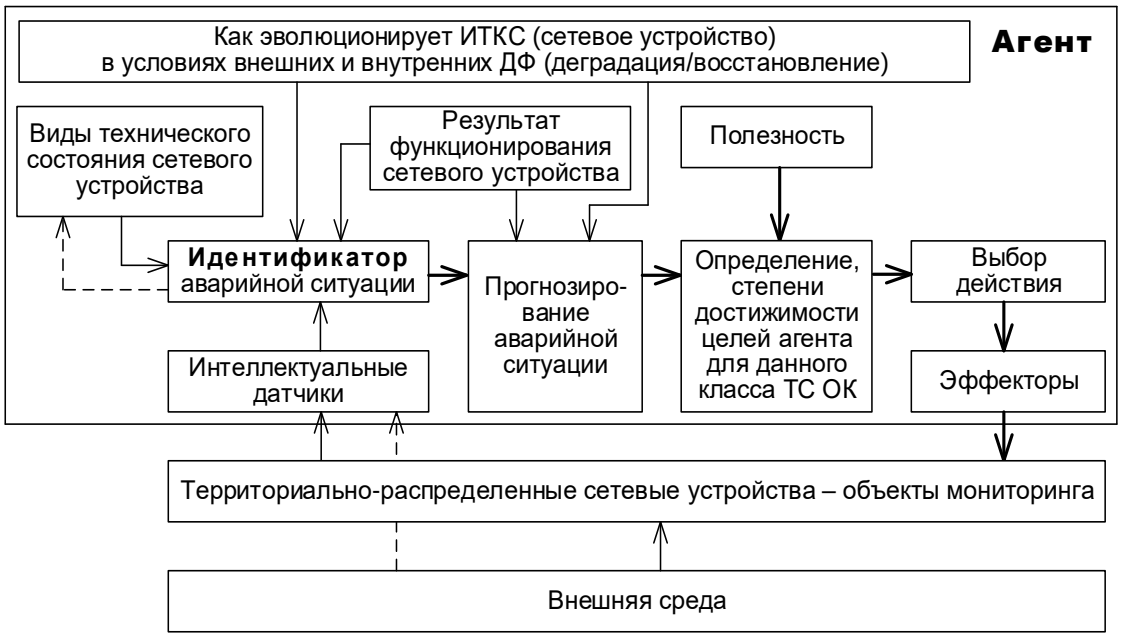

Рис. 2. Архитектура интеллектуального агента, основанная на оценке полезности действий [15]

При формировании модели подсистемы мониторинга на основе мультиагентного подхода вводим допущение, что один ИА владеет лишь частью информации, нужной для решения задачи в целом, а, следовательно, он может решить только некоторую часть задачи. Поэтому для выполнения задач мониторинга сетевых устройств на сегменте сети или ИТКС в целом, функциониру-

ющих в условиях ДФ, необходимо множество ИА увязать (сопрячь) между собой и обеспечить их необходимое взаимодействие, создав МАС, в которой множество задач по установленным правилам распределяется между отдельными ИА, каждый из которых входит в состав общей системы.

Каждый ИА, независимо от размещения на сетевых устройствах, физически представляет собой ЭВМ, работающую на различных логических уровнях ИТКС (рис. 1) под управлением операционной системы и комплекса информационно-технических средств (КИТС) сервера мониторинга, проводящего:

– текущее перераспределение сетевых устройств и каналов связи (постановку на мониторинг и снятие с него), реализуемое методами сбора, обработки, отображения и документирования измерительной информации, а также актуализации (репликации) баз данных (БД) и знаний (БЗ);
– сбор измерительной информации с различных автоматизированных измерительных комплексов (АИК) и интеллектуальных датчиков (ИД), интеллектуальной ИИС, установленных в подконтрольной агенту сети;
– обмен измерительной информацией между интеллектуальными агентами;
– выработка рекомендаций в интересах системы поддержки принятия управленческих решений (СППР) на переконфигурацию сети.

При этом на программном уровне каждый ИА представляет собой расчетные модули, предназначенные для: оценки ТС по ИИ от разных измерительных устройств; прогноза отказов; оптимизации режимов работы сети.

Динамика изменения ДФ, воздействующих на сетевые устройства и сегменты сети приводят в некоторых случаях к необходимости обмена информацией между ИА одного уровня, разделенными между собой резервными каналами ТИ-ТС. Логическая схема обмена ИИ по каналам ТИ-ТС может отличаться от физической схемы основных каналов информационного обмена на ИТКС. Каждый ИА хранит в себе лишь часть схемы сети и выполняет перерасчет ее режимов по мере поступления ИИ от измерительных устройств. Помимо этого, агенты содержат информацию о связях с другими ИА и передают им информацию о результатах вычислений соседних сегментов сети, на основе чего итерационно повторяются вычисления для уточнения результатов на текущее значение временного интервала. Критерием остановки обмена ИИ между ИА может быть либо предельно заданное число итераций, либо порог времени с момента первого расчета, или же достигнутый предел точности, который определяется как разница результатов между двумя итеративными расчётами.

Модель идентификации технического состояния сетевых устройств

При эксплуатации ИТКС ОП, построенных по многоуровневому принципу, работоспособность сетевых устройств всегда характеризуется достаточно большим количеством параметров, наблюдаемых с разных контуров управления, в связи с чем их мониторинг целесообразно осуществлять в несколько этапов [1, 5, 13, 14, 17]. К примеру, на начальном этапе по выбранному обобщенному показателю проводится проверка системы на работоспособность, а в случае обнаружения аномальной (аварийной, или предаварийной) ситуации, на следующем этапе осуществляется более тщательная проверка с использованием

ИИ локального (сервера мониторинга), регионального (подсистемы мониторинга) или глобального (ситуационного центра (СЦ) или АСУС) контура организации контроля и управления судят о ее реальном состоянии. Такая процедура мониторинга приводит к значительному сокращению как времени проверок, так и объемов циркулирующей в системе измерительной информации [18].

При решении задачи моделирования процесса идентификации технического состояния сетевых устройств будем исходить из того, что территориально распределенная ИТКС построена по иерархическое структуре, поэтому и модель ее подсистемы мониторинга должна позволять осуществление перераспределения функций мониторинга между центральным диспетчерским пунктом управления (ДПУ), размещаемым в сегменте мониторинга СЦ ведомства [19] и региональной подсистемы мониторинга ИТКС, либо сервером мониторинга на локальном уровне сети – ЛВС, в зависимости от текущего состояния системы с использованием агентно-ориентированного подхода [15]. При этом на первом этапе по локальной ИИ, определяется наличие нарушения режима работы ИТКС, а на втором и последующих этапах уточняется степень и тип нарушения на основных элементах ИТКС. Графовая вероятностная модель идентификации ТС сетевого устройства ИТКС приведена на рис. 3.

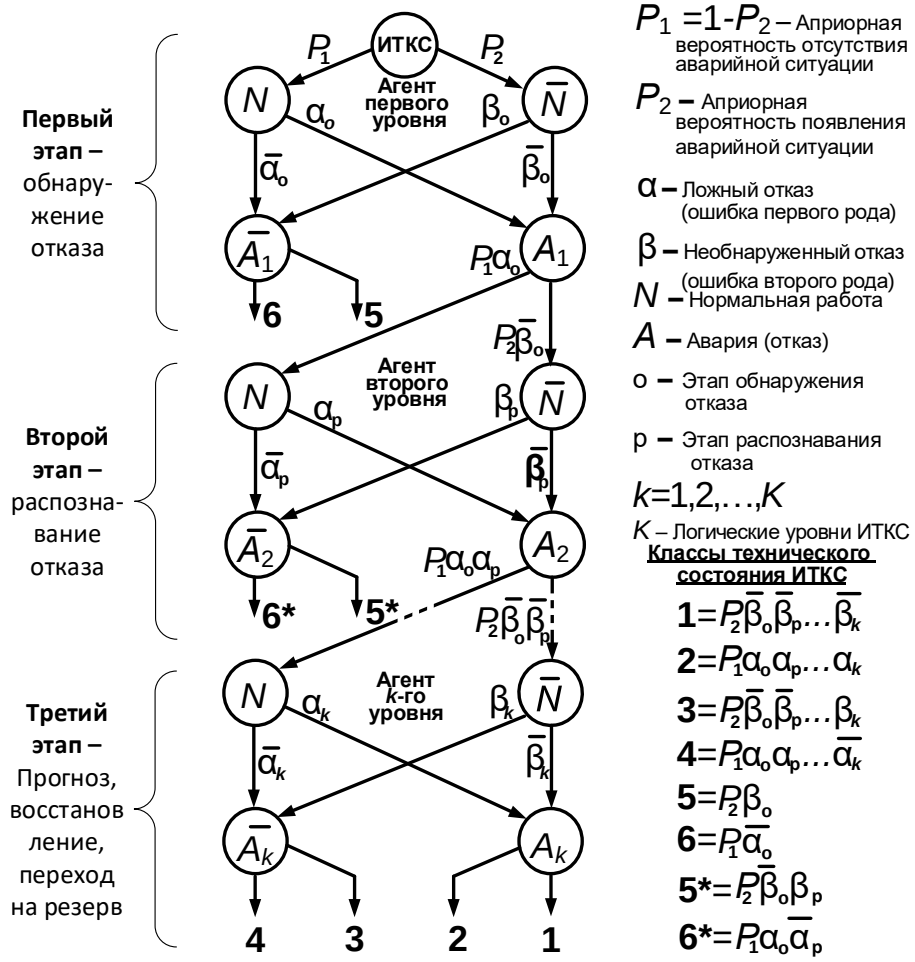

Рис. 3. Вероятностная модель идентификации вида технического состояния сетевого устройства

Графические модели широко применяют в теории вероятностей, в Байесовской статистике, а также в машинном обучении [1, 2, 13, 17]. На данной вероятностной модели в виде графа представлены зависимости между случайными величинами, характеризующими ТС элементов сети. Вершины графа соответствуют случайным переменным (видам ТС), а рёбра – вероятностным взаимосвязям между случайными величинами, где $P_1 = 1 - P_2$ – априорная вероятность отсутствия аварийной ситуации; P_2 – априорная вероятность появления аварийной ситуации; α – ошибка первого рода (ложный отказ); β – ошибка второго рода (необнаруженный отказ); N – нормальная работа; A – авария (отказ); о – этап обнаружения отказа; р – этап распознавания отказа; $k = 1, 2, ..., K$ – уровни ИТКС.

При выявлении неработоспособного (аварийного) либо предотказного (предаварийного) состояния сетевого устройства осуществляется рассылка интеллектуальных агентов, пронумерованных по уровням иерархии, которые управляют техническим состоянием сетевых элементов, приводя их в нормальное (состояние N на рис. 3) состояние (осуществляя переконфигурацию сети). Под аварийной (предаварийной) ситуацией понимается состояние сетевого устройства, сегмента сети или ИТКС в целом, при котором наблюдается отклонение метрик контролируемых параметров за пределы установленного допустимого порога $z^{\text{пор}}(k, n, m)$, (либо существенное приближение к значению заданного порога).

На основе использования теории статистических решений возможно найти метод, основанный на результатах анализа, который с минимальной вероятностью ошибки дает ответ на вопрос, к какому из двух множеств N или $\overline{N}$ относится наблюдаемой текущее техническое состояние сетевого устройства и соответствующий ему вектор, $S = S(x_1, x_2, \ldots, x_n)$. При этом в ходе применения решения классификации вида ТС всегда будут иметь место ошибки первого рода α, возникающие тогда, когда гипотеза $U_1(S = \overline{N})$ отклоняется, хотя была справедливой, а также ошибки второго рода β, возникающие тогда, когда оказывается справедливой гипотеза $U_1(S = \overline{N})$, но принимается гипотеза $U_2(S = N)$. Для осуществления идентификации вида ТС необходимо найти решающее правило (правило Байеса), которое минимизировало бы средний риск $W = \delta_a \cdot \alpha + \delta_b \beta$ [1, 13, 17], или среднюю стоимость принятия решения о наличии ошибок первого и второго рода, где δ_a и δ_b – соответственно веса ошибок первого и второго рода:

$$S \in N, \text{ если } \frac{P(x_1,...,x_n / N}{P(x_1,...,x_n / \overline{N})} > \frac{\delta_a P(\overline{N})}{\delta_b P(N)} = \theta;$$

$$S \in \overline{N}, \text{ если } \frac{P(x_1,...,x_n / N}{P(x_1,...,x_n / \overline{N})} << \frac{\delta_a P(\overline{N})}{\delta_b P(N)} = \theta,$$

где $P(x_1,..,x_n / N)$ и $P(x_1,...,x_n / \overline{N})$ – соответственно условные плотности вероятностей нормального функционирования и возникновения аварии ИТКС, которые формируются в процессе обучения системы, при этом необходимо допустить, что они близки к истинным, поскольку критерий (правило) Байеса обеспечивает наивысшую точность решения двуальтернативных задач распознава-

ния (идентификации) [17]; $P(\overline{N}) = 1 - P(N)$ – априорная вероятность возникновения аварии.

Тогда решающее критерий Байеса, минимизирующий средний риск *W*, сравнивает отношение вероятностей с неким порогом θ, являющимся постоянным для определенных значений весов δ_a и δ_b, а отношение

$$L(x_1,...,x_n) = \frac{P(x_1,...,x_n / N)}{P(x_1,...,x_n / \overline{N})},$$

называют отношением правдоподобия [17].

В процессе построения многомерной разделяющей границы порогов идентификации приходится использовать всю доступную измерению информацию, как при централизованном, так и при децентрализованном управлении. В первом случае вся ИИ, на основе которой принимается решение о работе элементов сети, собирается в подсистеме мониторинга СЦ, и в виде агентов (директив) рассылается по сети [20]. Во втором случае сама подсистема мониторинга ИТКС должен располагать достаточной априорной информацией для принятия обоснованного решения о состоянии не только всей сети, но и о состоянии всех ее элементов, во избежание аварии.

В связи с тем, что на каждом из этапов сервер мониторинга (подсистема мониторинга) может совершать ошибки первого рода $\alpha(x_{oi})$ и второго рода $\beta(x_{oi})$, то для нормального функционирования классификатора подсистемы мониторинга необходим выбор порогов x_{0i} на каждом из *i*-го этапов. Тогда с учетом введенных обозначений запишем [1, 17]:

$$\alpha(x_{0i}) = \int_{x_{0i}}^{\infty} f(x_i / N)dx_i ,$$

$$\beta(x_{0i}) = \int_{-\infty}^{x_{0i}} f(x_i / \overline{N})\, dx_i ,$$

а исходя из модели, представленной на рис. 3 и [1, 17] получим суммарные ошибки пропуска отказа $P_{\text{пр}}$ и ошибки ложной тревоги $P_{\text{лт}}$:

$$P_{\text{пр}} = P_2\left[1 - \prod_{i=1}^{n} \beta(x_{0i})\right] ; \quad (1)$$

$$P_{\text{лт}} = P_1 \cdot \prod_{i=1}^{n} \alpha(x_{0i}) . \quad (2)$$

Для получения оптимальных порогов классификации в соответствии с критерием Неймана-Пирсона зафиксируем вероятность ложной тревоги $P_{\text{лт}}$ на заданном уровне при минимизации ошибки пропуска отказа $P_{\text{пр}}^{\min}$, в которой переменные x_{0i} связаны функциональной зависимостью $P_{\text{лт}}$. Такая постановка задачи относится к задаче условной оптимизации с функционалом, выраженным с использованием неопределенного множителя Лагранжа λ [1, 17]:

$$\Phi = P_2\left[1 - \prod_{i=1}^{n} \beta(x_{0i})\right] + \lambda P \prod_{i=1}^{n} \alpha(x_{0i}) .$$

Рассчитав частные производные $\partial\Phi/\partial x_{0i}$, построим систему n уравнений, что совместно с уравнениями (1) и (2) позволит найти множитель λ и n переменных x_{0i}. После дифференцирования полученного результата в уравнениях искомыми являются оптимальные пороги классификации на каждом этапе $(x_{01}^*, x_{02}^*, ..., x_{0i}^*, ..., x_{0n}^*)$, с помощью которых минимизируется вероятность пропуска отказа $P_{\text{пр}}^{\min}$, связанная с минимальной вероятностью ошибки возникновения аварии. Данное решение позволяет однозначно рассчитать вероятность применения правильного решения об отсутствии отказа в работе сетевых элементов ИТКС: $\overline{P}_{\text{пр}} = 1 - P_{\text{пр}}^{\min}$.

На последующих этапах мониторинга анализу подвергается информация о принятии верного решения $\overline{\beta}_i = 1 - \beta_i$, т. е. об идентификации нормального функционировании сетевого устройства.

Предложенная на рис 3 модель подсистемы мониторинга фактически реализует поэтапную процедуру принятия решения, когда на первом этапе происходит *обнаружение* отказа критически важных элементов (КВЭ) сети, а на втором – его *распознавание* с использованием объектовых серверов мониторинга. Данные этапы условно показаны в виде обнаружителя и распознавателя. В предложенной вероятностной модели идентификации ТС сетевого устройства можно выделить финальные значения вероятностей его нахождения в том или ином техническом состояния. По этим финальным вероятностям ИТКС определяются классы ТС:

– «1» – ИТКС заблокирована, но возникший отказ обнаружен и распознан;
– «2» – ИТКС работоспособна, однако при этом произошло ложное обнаружение и распознание отказа;
– «3» – ИТКС заблокирована, при этом отказ обнаружен, но не распознан;
– «4» – ИТКС работоспособна, однако произошло ложное обнаружение отказа, которое не распознано;
– «5» – ИТКС заблокирована, но при этом отказ не обнаружен;
– «6» – ИТКС работоспособна и сервером мониторинга признана таковой.

Представленные на рис. 3 классы ТС «1-4» относятся к завершающему этапу работы подсистемы мониторинга ИТКС, а классы «5», «6», – к ее работе на каждом из уровней (этапов) функционирования ИТКС. При этом математически, данные классы ТС, согласно данной вероятностной модели, можно выразить как:

$$1 = P_2\overline{\beta}_o\overline{\beta}_p;\ 2 = P_1\alpha_o\alpha_p;\ 3 = P_2\overline{\beta}_o\beta_p;\ 4 = P_1\alpha_o\overline{\alpha}_p;\ 5 = P_2\beta_o;\ 6 = P_1\overline{\alpha}_o. \quad (3)$$

Для эксплуатанта сетевого оборудования и телеком-оператора наиболее предпочтительным являются класс ТС «6», когда ИТКС работоспособна и признана работоспособной. Далее по предпочтению идет класс «1» – система заблокирована, когда отказ обнаружен и распознан. Математически вариационный ряд предпочтений классов состояния ИТКС с учетом выражения (3) можно записать как:

$$\text{«6»} \succ \text{«1»} \succ \text{«4»} \succ \text{«2»} \succ \text{«3»} \succ \text{«5»}. \quad (4)$$

Представляя данный вариационный ряд предпочтений (4), имеется в виду предпочтения с точки зрения достоверности мониторинга. Класс состояния «6», когда система работоспособна и признана работоспособной, носит статус «подтвержденного» результата измерений [2] о исправности КВЭ или всей зоны мониторинга. При получении результата измерения в виде класса ТС «1» (система отказала, отказ обнаружен и распознан) подсистема мониторинга в автоматическом режиме должна выдать команду в систему поддержки принятия решений (СППР) по переходу на резервный комплект оборудования. При статусе «подтвержденного» результата измерений данные классы состояния сетевых элементов преобразуются серверами мониторинга в формализованный сигнал о виде ТС ОК. При этом по сети транслируется не вся доступная серверу мониторинга ИИ, а только вид ТС ОК: нормальное или аварийное состояния. Тем самым осуществляется значительное сокращение объемов передаваемой ИИ [18] в систему мониторинга сети и для репликации ее БД, БЗ.

Передача всей доступной ИИ на от сервера мониторинга в подсистему мониторинга более высокого логического уровня сети осуществляется только в случае определения вида ТС, отличного от «подтвержденных» статусов нормального функционирования или аварии, например, предотказное ТС, характеризуемое статусами «ориентирующий», «экстраполированный» и «недостоверный» [2]. На вероятностной модели рис. 3 данные состояния обозначены как «2», «3», «4», «5», характеризующие предотказное состояния ОК и требующие вмешательства оператора подсистемы мониторинга для принятия решения.

В некоторых случаях при распознавании аварийного состояния ОК после перевода его подсистемой мониторинга на резервную схему, или после переконфигурации сети (с изменением маршрутов передачи информации), подсистема мониторинга более высокого логического уровня может запросить у сервера мониторинга и всю доступную ИИ для детального анализа ситуации в процессе диагностики отказавшего КВЭ, поскольку для аудита неисправности и проведения перепрограммирования и тестовых проверок сетевого оборудования формализованного сигнала с классом его ТС явно недостаточно.

Поскольку сервер мониторинга работает в интересах подсистемы мониторинга распределенной ИТКС, как элемента СППР СЦ, а ошибки первого и второго рода могут возникать не только в сервере мониторинга, но и при передаче ИИ по каналам ТИ-ТС сети, то вероятностная модель идентификации вида ТС сетевого оборудования (рис. 3) может быть преобразована в многоэтапный вероятностный граф функционирования всей автоматизированной подсистемы мониторинга с учетом этапа передачи информации в СППР, см. рис. 4. На данном графе появляется еще один этап, на котором также могут иметь место ошибки первого и второго рода – этап прогноза состояния ИТКС путем перехода на резервные комплекты сетевого оборудования, переконфигурации сети и пр.

№5. 2021
ISSN 2410-9916

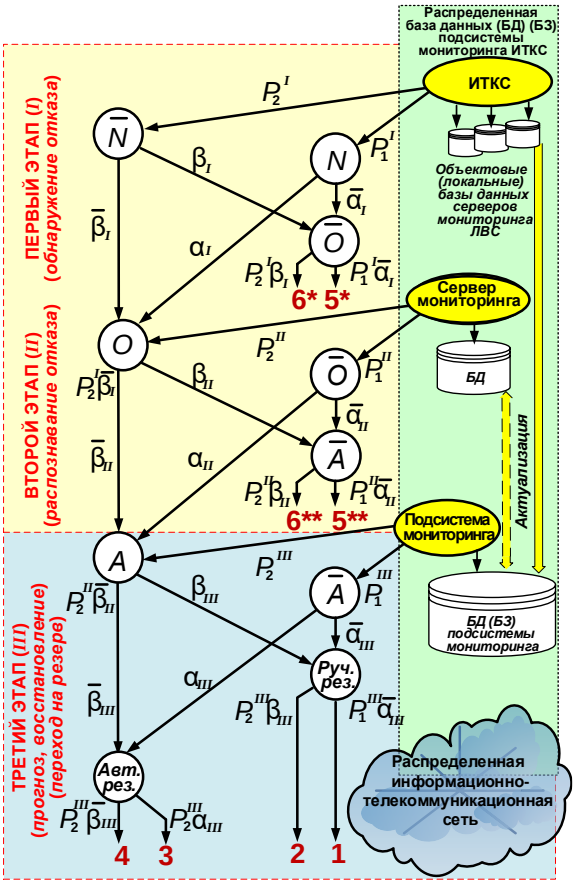

Рис. 4. Вероятностный граф функционирования подсистемы сетевого мониторинга ИТКС

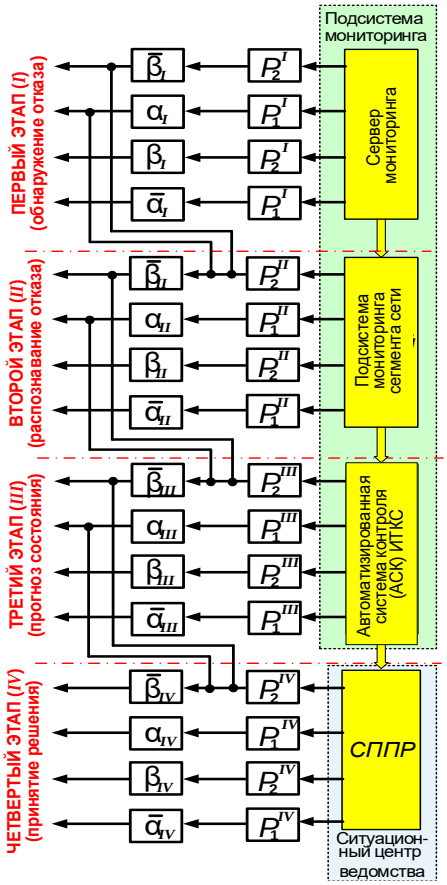

Рис. 5. Надёжностная схема замещения вероятностного графа функционирования подсистемы сетевого мониторинга ИТКС

При этом на рис. 4 и 5 дополнительно к введенным ранее, используются обозначения: Авт.рез. – автоматический переход на резервный комплект сетевого оборудования; Руч.рез. – ручное включение резерва оператором подсистемы мониторинга; *I*, *II*, *III*, *IV* – этапы процедуры идентификации состояния сетевого элемента (сети); «*» – вид состояния ИТКС на каждом этапе идентификации.

В этом случае надёжностная схема замещения вероятностного графа функционирования подсистемы сетевого мониторинга с учетом еще одного этапа принятия решения в СППР (на рис. 3 и 4 не показан) приведена на рис. 5.

Исходя из представленной модели и вероятностного графа, а также надежностной схемы замещения, рис. 3-5, вероятности идентификации подсистемой мониторинга работоспособного состояния ($P_{\text{рбт.с}}$) и, соответственно, неработоспособного состояния (отказа) $P_{\text{отк}}$ сетевого элемента будут равны:

$$P_{\text{рбт.с.}} = 1-\left(1-\bar{\beta}_{IV}\left\langle 1-\left[\bar{\beta}_{III}\left\{1-\left(1-P_1^{I}\alpha_I\bar{\beta}_{II}\right)\left(1-P_1^{II}\alpha_{II}\right)\right\}\right]\left[1-P_1^{III}\alpha_{III}\right]\right\rangle\right)\times$$

$$\times\left(1-P_1^{IV}\alpha_{IV}\right),$$

$$P_{\text{отк}} = \left(1-\left\langle 1-\bar{\beta}_{III}\left[1-\bar{\beta}_{II}\left\{1-\left(1-P_2^{I}\alpha_I\bar{\beta}_I\right)\left(1-P_2^{II}\right)\right\}\right]\left[1-P_2^{III}\right]\right\rangle\left\langle 1-P_2^{IV}\right\rangle\right)\bar{\beta}_{IV}\,.$$

DOI: 10.24412/2410-9916-2021-5-40-64
URL: https://sccs.intelgr.com/archive/2021-05/03-Allakin.pdf

Оценка результатов моделирования

При моделировании распределенной ИТКС и ее подсистемы мониторинга использован подход «сверху вниз», который позволяет учесть и рассмотреть проявление выхода параметров сетевых устройств за пределы допусков на разных логических уровнях сети, когда при нормальном ее функционировании распределенная структура просматривается широким оперативным полем при малой решающей способности, достаточной для обнаружения локального нарушения режима работы. При последующем анализе происходит сужение оперативного поля в области нарушения, которое контролируется детально и путем более тонкого анализа производится идентификация (распознавание) характера нарушения. Данная процедура проводится сервером мониторинга при анализе временных рядов метрик параметров подконтрольных сетевых элементов.

В связи с тем, что решение о нормальном функционировании ИТКС на первом этапе принимается на основе локальной информации о состоянии элементов сети (например, о состоянии исходящих каналов, загрузке процессора, занятом объеме буферной памяти, и пр.), то серверу мониторинга ЛВС нет необходимости обмена информацией с другими серверами сети и общей подсистемой мониторинга, что существенно сокращает объемы передаваемой по сети ИИ. На втором и последнем этапах мониторинга анализу подвергается та часть ИИ, которая обусловливает появление вероятностей ложной тревоги – $P_1\alpha_1$, $P_1\alpha_1\alpha_2$,…, $P_1\alpha_1\alpha_2$,…,α_n, и которая должна подвергаться дальнейшему анализу. Значение вероятности $P_{\text{лт}} = P_1\alpha_1(1 + \alpha_2 + \alpha_2\alpha_3 + \ldots + \alpha_2\alpha_3\ldots\alpha_n)$ определяет часть общего потока измерительной информации, подлежащей анализу на втором и последующих этапах мониторинга, и, соответственно, степень сокращения η_c объема ИИ, передаваемой между серверами мониторинга в подсети и внутри распределенной БД (БЗ) подсистемы мониторинга сети [1, 17]:

$$\eta_c = \frac{1}{P_1\alpha_1(1+\alpha_2+\ldots\alpha_2\alpha_3\ldots x_n)}.$$

Таким образом, степень сокращения объема ИИ, циркулирующей по ИТКС, зависит от величины ошибок первого рода на каждом из этапов мониторинга, осуществляемых на логических уровнях сети, рис. 1.

Заключение

Представленная модель идентификации технического состояния сетевого устройства подсистемой мониторинга в отличие от известных имеет иерархическую структуру и позволяет осуществлять перераспределение функций центра управления и периферии в зависимости от текущего состояния системы с использованием агентно-ориентированного подхода.

Достоинствами данной модели являются следующие:

1. Используемый при моделировании многоуровневый подход позволяет осуществлять более точную идентификацию функционального состояния сетевого элемента, когда на первом этапе по локальной информации, содержащейся в сервере мониторинга, определяется наличие нарушения режима работы, а на втором и последующих этапах уточняется степень и тип нарушения. Каждый этап связан с соответствую-

щим логическим уровнем сети. При выявлении аномальных ситуаций осуществляется рассылка интеллектуальных агентов, пронумерованных по уровням, которые управляют состояниями сетевых устройств, приводя их в нормальное состояние.

2. Поэтапная процедура мониторинга обеспечивает наивысшую точность выявления аномальных ситуаций на ИТКС, поскольку использует на каждом из этапов независимые признаки распознавания и, следовательно, оказывается не хуже байесовой. При такой процедуре применение решения о состоянии ИТКС осуществляют с привлечением дополнительных признаков по мере необходимости. Число включений этапов уменьшается по мере роста номера этапа в x_i раз. Процесс анализа в каждом цикле мониторинга завершается если принято решение о нормальном функционировании сети. Последние этапы используются редко, при этом суммарное количество ИИ в пределе достигает максимума, практически используя всю доступную измерению ИИ, поставляемую системой сетеметрии, для принятия окончательного решения.
3. Анализ результатов моделирования показывает, что выигрыш в отношении сокращения объема ИИ зависит от информативности признаков распознавания на втором и последующих этапах процедуры мониторинга в каждом его цикле, поскольку информативность признака на первом этапе (в сервере мониторинга) оказывается фиксированной (локальная информация о значениях метрик параметров каждого конкретного сетевого устройства). На втором и последующих этапах информативность признаков возрастает, что связано с измерениями на сети, проводимых как другими серверами мониторинга на основе фактических измерений в окружении – т. н. технология мобильного массового считывания (MCS – Mobile Crowd Sensind), так и непосредственно самой подсистемой мониторинга сегмента сети (подсети) или ИТКС (сегмент мониторинга ситуационного центра). Объем данных измерений определяет качество принятия решения СППР при поэтапном мониторинге (контроле). Однако, необходимо отметить, что эти измерения для повышения информативности связаны с необходимостью привлечения дополнительных измерительных ресурсов и естественным образом увеличивают время анализа, повышая точность принятия решения при ситуационном управлении по переконфигурации сети.
4. В случае идентификации «подтвержденных» статусов нормального функционирования сетевого устройства ИИ по сети не транслируется. При идентификации «подтвержденного» статуса отказа – передается формализованный сигнал на включение резерва (перемаршрутизацию). И только при идентификации предотказного ТС, характеризуемого статусами «ориентирующий», «экстраполированный» и «недостоверный» [2] осуществляют передачу всей доступной ИИ от системы сетеметрии и локального сервера мониторинга в подсистему мониторинга более высокого логического уровня сети, для принятия решения, направленного на предупреждение отказа.

Литература

1. Будко П. А., Кулешов И. А., Курносов В. И., Мирошников В. И. Инфокоммуникационные сети: энциклопедия. Кн. 4. Гетерогенные сети связи: принципы построения, методы синтеза, эффективность, цена, качество /под ред. проф. В. И. Мирошникова. – М.: Наука, 2020. – 683 с.

2. Виноградено А. М. Методология интеллектуального контроля технического состояния автоматизированной системы связи специального назначения. Монография. – СПб.: Наукоемкие технологии, 2020. – 180 с.

3. ГОСТ 27.002-2015. Надежность в технике. Термины и определения. – М.: Издательство стандартов. 2016. – 23 с.

4. ISO 9126:1991. Software enginnering – Product quality – 2000. – URL: https://www.cse.unsw.edu.au/~cs3710/PMmaterials/Resources/9126-1%20Standard.pdf. (дата обращения 03.09.2021).

5. Аллакин В. В., Будко Н. П. Идентификация состояния узлов информационно-телекоммуникационных сетей общего пользования подсистемой мониторинга информационной безопасности // Техника средств связи. 2020. № 3 (151). С. 58-64.

6. Каляев И. А. Реконфигурируемые вычислительные системы. – Ростов-на-Дону: Изд-во Южного федерального ун-та, 2016. – 472 с.

7. Recommendation ITU-T M.3703 Common management services. Alarm management. Protocol neutral requirements and analysis – URL: http://www.itu/int/rec/T-REC – M.3703 – 201006-1 (дата обращения 03.05.2021).

8. Евланов Л. Г. Контроль динамических систем. – М.: Наука, 1979. – 432 с.

9. Майданович О. В., Каргин В. А., Мышко В. В., Охтилев М. Ю., Соколов Б. В. Теория и практика построения автоматизированных систем мониторинга технического состояния космических средств. – СПб.: ВКА, 2011. – 219 с.

10. Виноградено А. М., Меженов А. В., Будко Н. П. К вопросу обоснования понятийного аппарата неразрушающего экспресс-контроля технического состояния оборудования системы связи и радиотехнического обеспечения аэродрома // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 6. С. 30-44. doi: 10.24411/2409-5419-2018-10293.

11. Абрамов О. В., Розенбаум А. Н. Управление эксплуатацией систем ответственного назначения. – Владивосток: Дальнаука, 2000. – 200 с.

12. Абрамов О. В. Планирование профилактических коррекций параметров технических устройств и систем // Информатика и системы управления. 2017. № 3 (53). С. 55-66.

13. Будко П. А., Рисман О. В. Многоуровневый синтез информационно-телекоммуникационных систем. Математические модели и методы оптимизации. – СПб.: ВАС, 2011. – 476 с.

14. Еремеев М. А., Аллакин В. В., Будко Н. П. Модель наступления критического события информационно-коммуникационной системе // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 6. С. 52-60.

15. Пузанков Д. В., Мирошников В. И., Пантелеев М. Г., Серегин А. В. Интеллектуальные агенты, многоагентные системы и семантический Web: концепции, технологии, приложения. – СПб.: ООО «Технолит», 2008. – 292 с.

16. ISO/IEC 7498-4: Системы обработки информации – Взаимное соединение открытых систем – Базовая справочная модель – Часть 4: Система управления – URL: http://ru.knowledgr.com/00402798/FCAPS (дата обращения 03.07.2021).

17. Фомин Л.А., Черноскутов А.И. Оптимизация ошибок при двухэтапной процедуре контроля // Автоматика и вычислительная техника. 1975. № 3. С. 34-37.

18. Будко Н. П. Сокращение объема измерительной информации на основе интеллектуального подхода к построению системы мониторинга информационно-телекоммуникационной системы // Техника средств связи. 2021. № 1 (153). С 86-97.

19. Зацаринный А. А., Шабанов А. П. Технология информационной поддержки деятельности организационных систем на основе ситуационных центров. – М.: ТОРУС ПРЕСС, 2015. – 232 с.

20. Клюев В. В., Соснин Ф. Р., Ковалев А. В. Неразрушающий контроль и диагностика: справочник / Под общ. ред. В. В. Клюева. – М.: Машиностроение, 2005. – 656 с.

References

1. Budko P. A., Kuleshov I. A., Kurnosov V. I., Miroshnikov V. I. *Infokommunikacionnye seti: enciklopediya. Kn. 4. Geterogennye seti svyazi: principy postroeniya, metody sinteza, effektivnost', tsena, kachestvo* [Infocommunication networks: an encyclopedia. Book 4. Heterogeneous communication networks: principles of construction, methods of synthesis, efficiency, price, quality]. Moscow, Nauka Publ., 2020. 683 p. (in Russian).

2. Vinogradenko A. M. *Metodologiya intellektual'nogo kontrolya tekhnicheskogo sostoyaniya avtomatizirovannoj sistemy svyazi special'nogo naznacheniya* [Methodology of intelligent control of the technical condition of an automated special-purpose communication system]. St. Petersburg, Naukoemkie tekhnologii Publ., 2020. 180 p. (in Russian).

3. State Standard 27.002-2015. Reliability in technology. Terms and definitions. Moscow, Standartov Publ., 2016. 23 p. (in Russian).

4. ISO 9126:1991. Software enginnering Product quality 2000. Available at: https://www.cse.unsw.edu.au/~cs3710/PMmaterials/Resources/9126-1%20Standard.pdf. (accessed 03 September 2021).

5. Allakin V. V., Budko N. P. Identification of the state of nodes of information and telecommunications networks of general use by the subsystem of information security monitoring. *Means of Communication Equipment*, 2020, no. 3 (151), pp. 58-64 (in Russian).

6. Kalyaev I. A. *Rekonfiguriruemye vychislitel'nye sistemy* [Reconfigurable computing systems]. Rostov-on-Don, Southern Federal University Publ., 2016. 472 p. (in Russian).

7. Recommendation ITU-T M. 3703 Common management services. Alarm management. Protocol neutral requirements and analysis Available at: http://www.itu/int/rec/T-REC-M.3703-201006-1 (accessed 30 July 2021).

8. Evlanov L. G. *Kontrol' dinamicheskih sistem* [Control of dynamic systems]. Moscow, Nauka Publ., 1979. 432 p. (in Russian).

9. Maidanovich O. V., Kargin V. A., Myshko V. V., Okhtilev M. Yu., Sokolov B. V. *Teoriya i praktika postroeniya avtomatizirovannyh sisem monitoringa tekhnicheskogo sostoyaniya kosmicheskih sredstv* [Theory and practice of building automated systems for monitoring the technical condition of space vehicles]. St. Petersburg, Military Space Academy named after A. F. Mozhaisky. 2011. 219 p.

10. Vinogradenko A. M., Mezhenov A. V., Budko N. P. To the question of substantiation of the conceptual apparatus nondestructive express control of technical condition equipment of communication system and aerodrome radio engineering support. *H&ES Research*, 2019, vol. 11, no. 6, pp. 30-44. doi: 10.24411/2409-5419-2018-10293 (in Russian).

11. Abramov O. V., Rosenbaum A. N. *Upravlenie ekspluataciej sistem otvetstvennogo naznacheniya* [Management of the operation of responsible purpose systems]. Vladivostok, Dal'nauka Publ., 2000. 200 p. (in Russian).

12. Abramov O. V. *Planirovanie profilakticheskih korrekcij parametrov tekhnicheskih ustrojstv i sistem* [Planning of preventive corrections of parameters of technical devices and systems]. *Informatics and control systems*, 2017, no. 3 (53), pp. 55-66 (in Russian).

13. Budko P. A., Risman O. V. *Mnogourovnevyy sintez informatsionno-telekommunikatsionnykh sistem. Matematicheskiye modeli i metody optimizatsii* [Multilevel synthesis of information and telecommunications systems. Mathematical models and optimization methods: A monograph]. St-Petersburg, Military Academy of Communications, 2011, 476 p. (in Russian).

14. Yeremeyev M. A., Allakin V. V., Budko N. P. Model of onset of the critical event of information security in information communication system. *H&ES Research*, 2017, vol. 9, no. 6, pp. 52-60 (in Russian).

15. Puzankov D. V., Miroshnikov V. I., Panteleev M. G., Seregin A. V. *Intellektual'nye agenty, mnogoagentnye sistemy i semanticheskij Web: koncepcii, tekhnologii, prilozheniya* [Intelligent agents, multi-agent systems and semantic Web: concepts, technologies, applications]. St. Petersburg, Technolit Publ., 2008. 292 p. (in Russian).

16. ISO/IEC 7498-4: Sistemy obrabotki informacii – Vzaimnoe soedinenie otkrytyh sistem – Bazovaya spravochnaya model' – Chast' 4: Sistema upravleniya [Information processing systems-Interconnection of open systems-Basic reference model-Part 4: Control system]. Available at: http://ru.knowledgr.com/00402798/FCAPS (accessed 03 July 2021) (in Russian).

17. Budko N.P. Reducing the amount of measurement information based on an intelligent approach to build a monitoring system for an information and telecommunications system. *Means of Communication Equipment*, 2021, no. 1 (151), pp. 86-97 (in Russian).

18. Fomin L. A., Chernoskutov A. I. Optimizaciya oshibok pri dvuhetapnoj procedure kontrolya [Error optimization in a two-stage control procedure]. *Automation and computer technology*, 1975, no. 3, pp. 34-37 (in Russian).

19. Zatsarinny A. A., Shabanov A. P. *Tekhnologiya informacionnoj podderzhki deyatel'nosti organizacionnykh sistem na osnove situacionnykh centrov* [Technology of information support for the activities of organizational systems based on situational centers]. Moscow, Torus Press Publ., 2015, 232 p. (in Russian).

20. Klyuev V. V., Sosnin F. R., Kovalev A. V. *Nerazrushayuschiy kontrol i diagnostika: spravochnik* [Non-destructive testing and diagnostics: reference]. Moscow, Mechanical Engineering Publ., 2003. 656 p. (in Russian).

Статья поступила 01.10.2021

Информация об авторе

Аллакин Владимир Васильевич – соискатель ученой степени кандидата технических наук. Независимый специалист. Область научных интересов: мониторинг информационных ресурсов; сбор и обработка информации. E-mail: vladimir@duduh.ru

Адрес: 188660, Ленинградская обл., Всеволожский район, пос. Бугры, ул. Школьная, д. 11, корп. 1, кв. 510.

A model for identifying the technical condition of information and telecommunication network devices by a network monitoring subsystem

V. V. Allakin

Task statement: *to substantiate the modeling of identification of the main types of technical condition of devices of public information and telecommunication networks based on methods of system analysis and a multi-level approach to the description of complex technical systems.* ***The purpose of the work:*** *to develop a model for identifying the technical condition of information and telecommunication network devices by a network monitoring subsystem in order to increase the efficiency of its functioning at various logical levels.* ***Methods used:*** *models of multi-agent (multi-agent) systems of intellectual decision support, methods of multilevel synthesis of complex technical systems, methods of reliability theory (functional control, monitoring, controlling), methods of classification theory, methods of identification of the type of state of a technical device based on the Neumann-Pearson criterion, methods of graph theory.* ***The novelty*** *of the study lies in the fact that the proposed model for identifying the technical condition of a network device by a monitoring subsystem, unlike the known ones, has a hierarchical structure, on the basis of which it allows for the redistribution of the functions of the network control center and peripherals depending on the current state of the system using an agent-oriented approach. At the same time, six classes of the technical condition of the network device are justified and described analytically, taking into account control errors of the first and second kind.* ***The result*** *of the conducted research consists in obtaining mathematical expressions to assess the probability of a functional state and the probability of failure of a network device in the process of multistage decision-making involving not only a monitoring server at the local level of the network hierarchy, but also a monitoring subsystem of a higher (regional) logical level and the entire information and telecommu-*

nications system as a whole. The multilevel approach used in modeling allows for more accurate identification of the functional state of a network element, when at the first stage, the presence of a violation of the operating mode is determined from the local information contained in the monitoring server, and at the second and subsequent stages, the degree and type of violation is specified. Each stage is associated with a corresponding hierarchy level. When abnormal situations are detected, intelligent agents are distributed, numbered by hierarchy levels, which control the states of network devices, bringing them to a normal state.

Keywords*: information and telecommunication network, monitoring subsystem, logical level, errors of the first and second kind, monitoring server, identification.*

Information about Author

Vladimir Vasilyevich Allakin – Doctoral Student. An independent specialist. Field of research: information monitoring; data acquisition. E–mail: vladimir@duduh.ru

Address: 188660, Russia, Leningrad region, Vsevolozhsky district, vil. Buhry, Shkolnaya str., 11, build. 1, sq. 510.