УДК 621.391

Концептуальная модель подсистемы интеллектуального мониторинга состояния информационно-телекоммуникационной сети общего пользования

Будко Н. П.

Постановка задачи: *на основе многоуровневого подхода к описанию сложных технических систем обосновать концептуальное моделирование подсистем сетевого мониторинга нового поколения.* ***Цель работы:*** *сформировать принципы построения и функционирования подсистемы интеллектуального мониторинга информационно-телекоммуникационной сети, общую структуру и обобщенную архитектуру перспективной системы сетевого мониторинга, а также разработать ее концептуальную модель в терминах многоуровневого синтеза подсистем контроля и диагностики.* ***Используемые методы:*** *методы многоуровневого синтеза сложных технических систем; модели и методы теории надежности; методы объектно-субъектного описания информационно-телекоммуникационных систем; реализации функциональной модели управления применительно к подсистемам мониторинга: управление отказами, управление конфигурацией, управление ресурсами, управление производительностью, управление безопасностью; методы моделирования метасистемы; методы представления знаний в сложных иерархических системах.* ***Новизна*** *исследования состоит в том, что в ходе концептуального моделирования сформулированы общие принципы функционирования перспективной подсистемы мониторинга; сформирована ее структура, включающая сенсорный, телекоммуникационный и диспетчерский уровни ее построения в системном аспекте; предложена обобщенная архитектура с компонентом интеллектуальной обработки, включающая модули онлайн-анализа, оффлайн-анализа и модуля поддержки и принятия решений.* ***Результат*** *проведенного исследования состоит в том, что представленная в работе совокупность требований и общих принципов функционирования перспективной подсистемы мониторинга, ее структуры, в терминах технических и технологических основ построения, а также архитектуры, общей модели подсистемы сетевого мониторинга и ее обобщенной модели представления знаний может рассматриваться как концептуальная модель подсистемы интеллектуального мониторинга нового поколения на сетевых инфраструктурах.*

Ключевые слова: *информационно-телекоммуникационная сеть, подсистема мониторинга, логический уровень сети, метамодель многоуровневой системы, модель знаний, зона мониторинга.*

Введение

На современном этапе развития информационно-телекоммуникационных систем и сетей (ИТКС) общего пользования (ОП) [1] в процессе их функционирования возникает ряд нерешенных задач, среди которых важное место занимает задача своевременного (в режиме реального времени или близкого к нему) получения достоверной информации о состоянии территориально-распределенной ИТКС, необходимой для организации процессов управления сетью связи как со стороны телеком-оператора (системного администратора), так и автоматизированной системой (АСУС). В значительной степени на решение данной

Библиографическая ссылка на статью:
Будко Н. П. Концептуальная модель подсистемы интеллектуального мониторинга состояния информационно-телекоммуникационной сети общего пользования // Системы управления, связи и безопасности. 2021. № 5. С. 65-119. DOI: 10.24412/2410-9916-2021-5-65-119

Reference for citation:
Budko N. P. Conceptual model of the subsystem of intelligent monitoring of the state of a public information and telecommunications network. *Systems of Control, Communication and Security*, 2021, no. 5, pp. 65-119 (in Russian). DOI: 10.24412/2410-9916-2021-5-65-119

задачи оказывает влияние то, как организована подсистема мониторинга и какова ее структура [2]. Поэтому вопросы формирования структуры подсистемы сетевого мониторинга являются исключительно *актуальными*.

Известны некоторые работы [3, 4] где рассматривается организация процедуры мониторинга ИТКС, однако вопросы формирования структуры и архитектуры подсистемы мониторинга практически не освещены. При этом важно создать (синтезировать) эффективные оперативные подсистемы, которые обеспечат получение необходимых для системы поддержки принятия решения (СППР) или АСУС достоверных данных о состоянии как всей ИТКС в целом, так и данных о состоянии всех ее компонент и элементов, а также протекающих в них процессах. При этом должна проявиться именно информационная (информационно-аналитическая) сущность подсистемы мониторинга, поскольку фактически каждая подсистема мониторинга глобальной сети, ее регионального сегмента, или сервера мониторинга в локальной сети, по сути является системой, создающейся для реализации операций анализа измерительной информации (ИИ) или данных, к которым можно всецело отнести операции сбора, получения, передачи, хранения, обработки, представления, поиска и использования ИИ на территориально-распределенной системе, что далеко не тривиально.

По мере эволюции направлений теории контроля и диагностики, технология создания подсистем мониторинга появилась из методов проведения *функционального контроля*. Это связано с тем, что обеспечение своевременного предотвращения развития аварийной ситуации на распределенной ИТКС возможен только проведением непрерывного либо периодического функционального контроля, что можно рассматривать по определению, соответственно, как *мониторинг* или *контроллинг* [5, 6]. Другие виды контроля (контроль готовности, контроль поисковый) при мониторинге не применимы, поскольку не относятся к методам режима реального времени, и используются как инструментальные методы контроля перед применением изделия по назначению и периодически в режимах ожидания использования, хранения или транспортирования, а также в ходе проведения различных видов технического обслуживания (ТО) и ремонтов (диагностики). При этом современные подсистемы мониторинга должны создаваться как комплексные системы, где реализуются большое число информационных процессов, протекающих в сетевых элементах (сетевых устройствах, в каналах (на маршрутах, на путях), в подсетях) и участвуют не только должностные лица телеком-оператора, но и оперативный состав органов управления – лица принимающие решение (ЛПР) на переконфигурацию ИТКС с целью недопущения развития негативных событий, заключающихся в перерастании предотказного состояния сети, в неработоспособное или предельное состояние [5] по причине воздействия внешних (ошибки обслуживающего персонала, условия эксплуатации, деструктивные воздействия и пр.) и внутренних (изменение режимов работы, величины генерируемого и обрабатываемого трафика и др.) дестабилизирующих факторов (ДФ). Именно от того, как построена подсистема мониторинга, и на каких принципах она функционирует в условиях ДФ, зависит качество процессов мониторинга и, в конечном виде, качество самого управления инфокоммуникационной системой со стороны СППР (АСУС).

Цель статьи: на основе системного анализа процессов контроля состояния территориально распределенной сетевой инфраструктуры сформировать общие принципы построения и функционирования подсистемы интеллектуального мониторинга ИТКС ОП, общую структуру и обобщенную архитектуру перспективной системы сетевого мониторинга, а также разработать ее концептуальную модель в терминах многоуровневого синтеза подсистем контроля и диагностики нового поколения.

Представление территориально-распределенной ИТКС ОП и ее подсистемы мониторинга с позиций многоуровневого подхода к моделированию

Активное использование на современном этапе развития общества информационных технологий (ИТ) опирается на широкое проникновение во все сферы производства и общественной жизни ИТКС ОП и систем разной сложности. Это привело к тому, что любые сбои и отказы на ИТКС ведут к существенным потерям от их простоев, выводя на первый план для телекоммуникационной отрасли задачи обеспечения надежности функционирования сетевых элементов и нивелирования дестабилизирующих воздействий среды распространения информационных сигналов (каналов связи). С целью оперативного выявления критических и аварийных (аномальных) ситуаций, а также сокращения времени их устранения на ИТКС в последние годы много внимания уделяется вопросам построения автоматизированных систем мониторинга, обеспечивающих постоянное наблюдение и периодический анализ изменения технического состояния сетевых элементов. Так, в соответствии с докладом ACFE, организации, применяющие в повседневной деятельности инструменты мониторинга и прогноза [7] в ИТ системах снижают свои потери на 60 % по сравнению с организациями, их игнорирующими.

При разработке систем сетевого мониторинга на ИТКС исследуемые характеристики отклонения эксплуатационных параметров от нормы возможно получить как в результате процедур пассивного мониторинга, применяя встроенную систему контроля сетевого элемента, или дистанционно на сервере мониторинга путём активного опроса периферии с помощью агентного подхода [8], когда в качестве интеллектуальных агентов используются управляющие пакеты, реализующие управление техническим состоянием (ТС) сетевых элементов, переводя их на резерв или приводя в нормальный режим функционирования. Причем встроенная система контроля (мониторинга) функционирует на локальном уровне системы, и в интересах периферийного устройства определяет «аномальное» ТС относительно «нормального» его состояния на основе статистических данных характеристик (параметров) сетевого элемента. В то время как сервер мониторинга, просматривая систему широким оперативным полем (на основе агентного подхода) способен решать проблемы функциональной безопасности всей ИТКС, не допуская ее блокировки, снижения уровня надежности и деградации.

Представим ИТКС в виде территориально-распределенной системы, имеющей иерархическую структуру и позволяющей осуществлять перераспределение функций мониторинга (сервера мониторинга) в зависимости от теку-

щего на данный момент времени состояния системы (ее сетевых элементов), рис. 1. Такое видение структуры ИТКС позволяет уйти от строгой централизации управления сетью к децентрализованному управлению. Действительно, управление глобальной системой, такой как ИТКС, не может быть строго централизованным в силу задержек, изменений текущего состояния сети и огромного потока управляющей информации (из опыта эксплуатации сети ARPA в конце 60 годов прошлого века в США – сеть блокировалась только за счет огромного объема управляющей информации без поступления реальной нагрузки). В алгоритмах работы современных сетей связи производительность системы зависит от принимаемых решений, которые принимаются с учетом текущего состояния сети, её деградации и дестабилизирующих воздействий внешней среды. В связи с этим, возникает самостоятельная задача динамического управления системой.

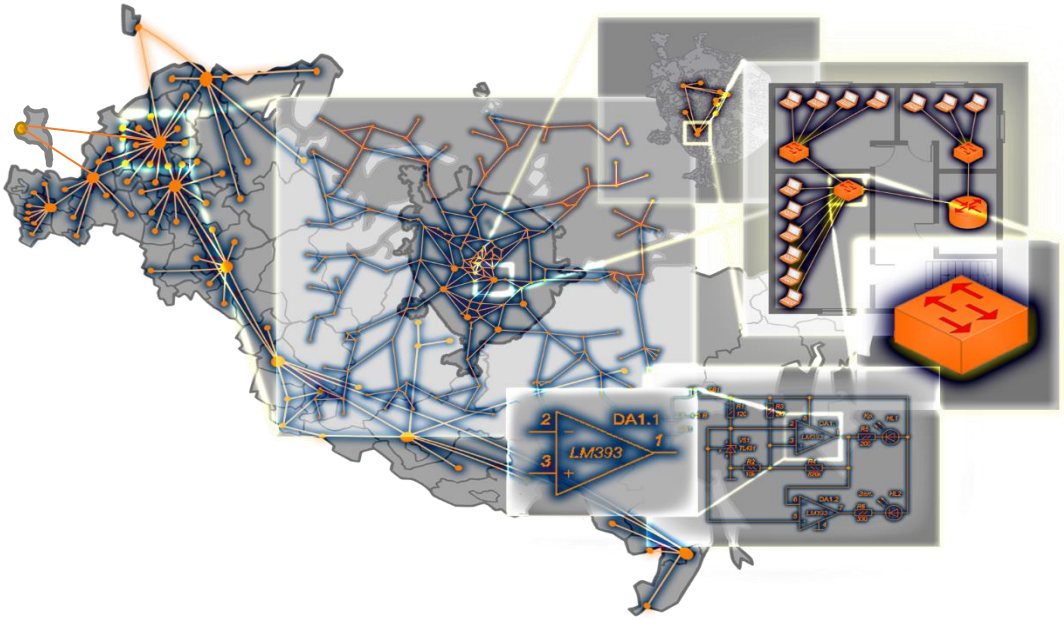

Рис. 1. Уровни разукрупнения информационно-телекоммуникационной системы

Представление ИТКС в таком виде (рис. 1) позволяет реализовать поэтапный процесс мониторинга, когда на первом этапе по локальной измерительной информации о состоянии периферии определяется наличие нарушения режима работы, а на втором и последующих этапах уточняется степень и тип нарушения. При этом каждый из этапов связан с соответствующим уровнем иерархии сетевой структуры (ИТКС). При обнаружении аномалии в изменениях значений контролируемых параметров сетевых элементов и каналов связи осуществляется рассылка интеллектуальных агентов (ИА), имеющих нумерацию по уровням иерархии ИТКС.

Учитывая территориальную рассредоточенность и зачастую автономность функционирования телекоммуникационного оборудования в Министерстве транспорта Российской Федерации (Минтрансе РФ), определяющие принципы, требования и архитектуру систем управления им, представление процесса мониторинга ТС объектов контроля (ОК) в работе будем рассматривать на

отдельных соответствующих подуровнях: *сенсорном*, *телекоммуникационном* и *диспетчерском*. А учитывая многоуровневость структуры ИТКС, на которой должна быть развернута перспективная подсистема мониторинга, ее ресурсы рассмотрим применительно к различным уровням функционирования эталонной модели взаимодействия открытых систем (ЭМВОС) OSI: физическому, канальному, сетевому, транспортному, сеансовому, представления и приложений.

Тогда типовой процесс мониторинга ТС сетевого оборудования *на сенсорном уровне* подсистемы мониторинга представляется в виде поступления сигналов с преобразователей (сенсоров, датчиков), характеризующих выход контролируемых параметров ОК за пределы допусков, на «элемент сравнения», представляющий собой компаратор или микроконтроллер, затем проведении сбора аналогичных сигналов с других объектов мониторинга в сенсорных узлах (узлах коммутации) и их селекции (ранжирования) по приоритету с учетом дестабилизирующих воздействий (внешняя и внутренняя среда функционирования, режимы работы). С точки зрения многоуровневого подхода, элементы сети, как объекты мониторинга, расположены на физическом уровне OSI (ЭМВОС) и сенсорном уровне моделируемой подсистемы мониторинга. Под ресурсами сенсорного уровня здесь будем понимать средства подсистемы мониторинга, используемые для регистрации отказов и формирования на их основе результатов оценки аварийных сигналов (интеллектуальные датчики, средства измерения и пр.). Примерами ресурсов данного уровня являются приборы, встраиваемые в объекты мониторинга: датчики, сенсоры, контроллеры и пр., а также время, затрачиваемое на процесс мониторинга. Учитывая, что критерием работоспособного состояния сетевого устройства является соответствие всех параметров, характеризующих способность выполнять заданные функции, требованиям нормативно-технической документации (НТД) [9], то в дальнейшем ресурсы, затрачиваемые на контроль функционирования объектов мониторинга на сенсорном уровне будем называть «параметрическим ресурсом», рис. 2.

Процесс преобразования и передачи аварийных сигналов (телеметрической информации – ТМИ) по линиям связи, с учетом внешних воздействий на среду передачи, представлен на *телекоммуникационном уровне* моделируемой подсистемы мониторинга. Ресурс, потребляемый подсистемой мониторинга на телекоммуникационном уровне, представляет собой каналы линий связи на канальном уровне и узловые функции, реализуемые средствами сетей (подсетей) на сетевом уровне, а также маршруты и пути доставки (транспортировки) пакетов ИИ от сенсоров (датчиков) к серверу мониторинга или заинтересованным группам пользователей диспетчерского пункта управления (ДПУ) из конца в конец на транспортном уровне модели OSI. Примерами ресурсов телекоммуникационного уровня подсистемы мониторинга ИТКС является сигнальный, энергетический и временной ресурсы на каналах ТМИ и сетях связи различного рода: радио, радиорелейные, космические, проводные, волоконно-оптические и др. Соответственно ресурсы, затрачиваемые на контроль функционирования объектов мониторинга на телекоммуникационном уровне будем называть «телекоммуникационным ресурсом», рис. 2.

№5. 2021
ISSN 2410-9916

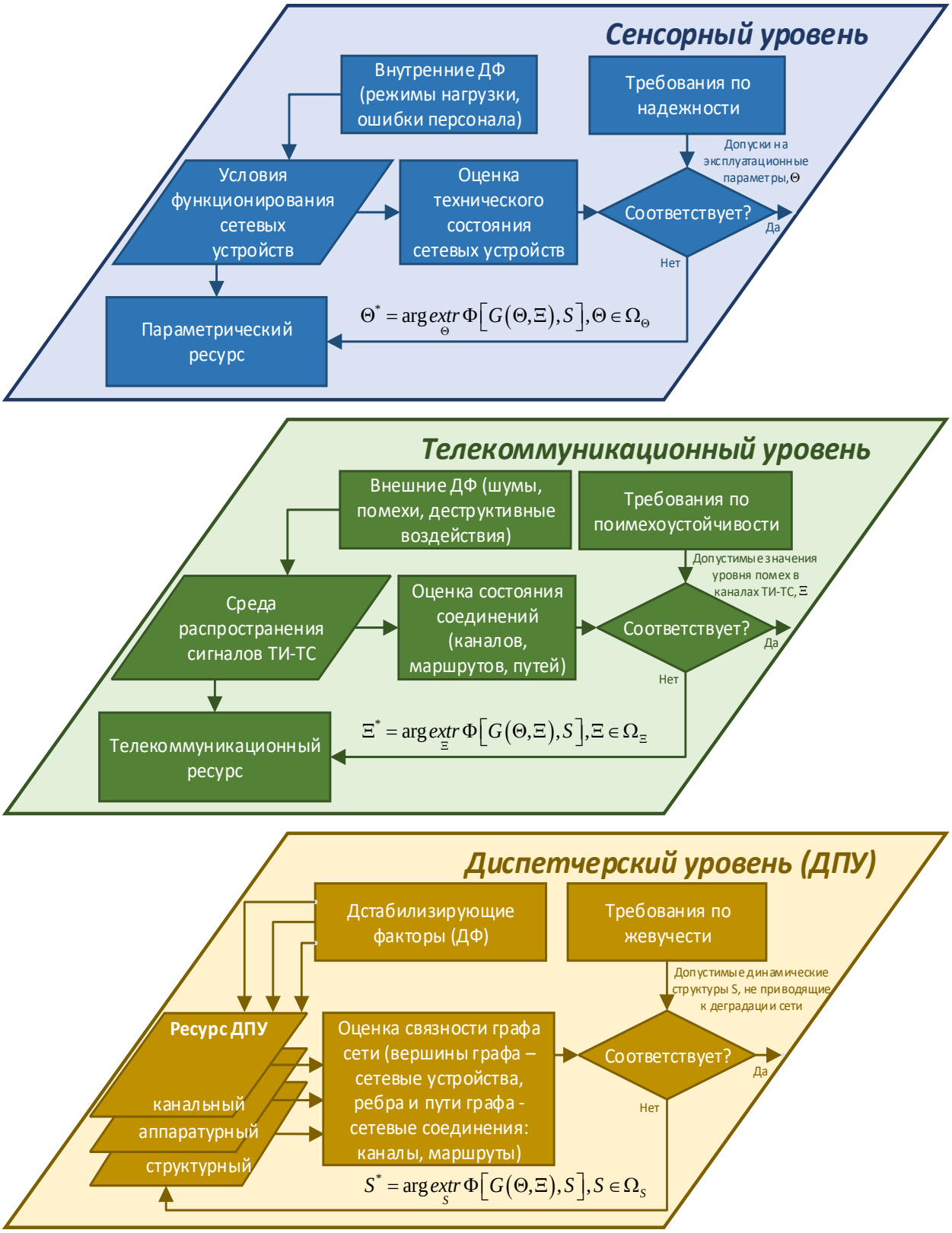

Рис. 2. Многоуровневый подход к процессу мониторинга состояния ИТКС ОП

Под *диспетчерским уровнем* моделируемой подсистемы мониторинга будем понимать ситуационный центр (или центр (пункт) управления связью) где осуществляется сбор и общий анализ поступающей ТМИ для принятия оперативных решений (ПОР) по связи на ИТКС. На диспетчерском уровне функционирования подсистемы мониторинга, формой потребляемых ресурсов являются

DOI: 10.24412/2410-9916-2021-5-65-119
URL: https://sccs.intelgr.com/archive/2021-05/04-Budko.pdf

локальные и удаленные терминалы (сервера мониторинга, комплексы управления функционированием (КУФ) и другое оборудование сегментов мониторинга ситуационных центров (СЦ) ведомств и отдельных корпораций (предприятий), а также автоматизированных систем управления технологическими процессами (АСУ ТП), для телекоммуникационной отрасли – АСУС) закрепленные через каналы передачи ТМИ за объектами мониторинга. Соответственно диспетчерский уровень подсистемы мониторинга охватывает сеансовый уровень, уровни представления и прикладной уровень модели OSI с его Web-интерфейсами отображения результатов мониторинга (ИИ) на серверах мониторинга коллективных табло отображения СЦ. Соответственно канальный, аппаратурный и вычислительный ресурсы, затрачиваемые на диспетчерском уровне подсистемы мониторинга ИТКС (на диспетчерском пункте управления) будем называть «ресурсом ДПУ», рис. 2.

Стратегия поддержания функциональной безопасности ИТКС при воздействии ДФ – это принятие оперативных решений на основе данных, полученных от подсистемы сетевого мониторинга, функционирование которой с учетом формирования и обновления данных в базах данных (БД) и базах знаний (БЗ) для ПОР осуществляется также с учетом дестабилизирующих воздействий, влияющих как на ОК, так и на саму подсистему сетевого мониторинга. Представляет интерес возможность подсистемы в процессе функционирования осуществлять самоподстройку (адаптацию) под имеющиеся условия, не снижая при этом показатели качества процесса мониторинга.

Любой сетевой элемент, как технический объект можно представить в виде $G = \{\Theta, \Xi\}$, где $\Theta = (\theta_1, \theta_2, \ldots, \theta_m)$ – параметры, а Ξ – условия эксплуатации объекта (в процессе контроля). Тогда, критерий качества функционирования подсистемы мониторинга можно задать в виде функционала $\Phi = \Phi(G, S)$, где S – структура подсистемы сетевого мониторинга. Таким образом, интеллектуальным мониторингом называется такая стратегия, которая всякую пару $\Phi = \Phi(G, S)$ приводит к цели – правильной идентификации состояния ИТКС и ее элементов.

Задача синтеза сводится к решению одной из оптимизационных задач:

$$\Theta^* = \arg \underset{\Theta}{\operatorname{extr}} \Phi[G(\Theta,\Xi), S], \ \Theta \in \Omega_\Theta, \quad (1)$$

$$\Xi^* = \arg \underset{\Xi}{\operatorname{extr}} \Phi[G(\Theta,\Xi), S], \ \Xi \in \Omega_\Xi, \quad (2)$$

$$S^* = \arg \underset{S}{\operatorname{extr}} \Phi[G(\Theta,\Xi), S], \ S \in \Omega_S, \quad (3)$$

где Ω_Θ, Ω_Ξ, Ω_S – допустимые множества, в рамках которых могут варьироваться соответственно параметры сетевых элементов, их условия эксплуатации (и отчасти условия эксплуатации подсистемы мониторинга), а также структура подсистемы мониторинга ИТКС, определяемые параметрическими, телекоммуникационными ресурсами и ресурсами ДПУ.

Исходя из этого, в работе используется совокупность трех групп показателей (Φ – показатели требований к качеству функционирования подсистемы мониторинга, Ξ – показатели внешних условий функционирования системы «сетевой элемент – сервер мониторинга», Ω – показатели ресурсов (параметри-

ческого, телекоммуникационного и ресурса ДПУ), применяемых при мониторинге состояния сетевых элементов в процессе их функционирования.

Перечисленные три группы показателей имеет двойственную структуру, позволяющую в зависимости от решаемой задачи одни показатели фиксировать в качестве ограничений, как исходные данные, а другие – задавать в качестве рассчитываемых показателей качества и эффективности. Это позволяет последние из них выделить в особую группу рассчитываемых показателей, которую обозначим показателями качества подсистемы мониторинга Q.

Связующим звеном между основными этапами (шагами) процесса мониторинга состояния сетевых элементов в соответствии с принятой стратегией мониторинга и различными видами элементарных циклов мониторинга, совокупность которых позволяет сформировать процедуру интеллектуального мониторинга в целом, являются алгоритмы выбора методов контроля и распределения ресурсов Ω подсистемы мониторинга. Выбор того или иного алгоритма определяется видом и степенью неоднородности ОК, степенью его автономности, оперативностью процедуры мониторинга, объемом проводимых операций, достоверностью и оценкой информации о состоянии сетевых элементов и ИТКС в целом, среды их функционирования, а также о наличии ресурсов, ограничивающих область принятия решений. Важно отметить, что адаптивность алгоритма мониторинга означает, что цель обеспечивается на всем классе объектов мониторинга и функционалов принятия решений. При этом в процессе контроля, вообще говоря, остается неизвестным, с помощью какого именно ресурса из допустимых множеств (Ω_Θ, Ω_Ξ, Ω_S) осуществляется мониторинг [10].

Внутренние характеристики системы «объект мониторинга – сервер мониторинга» можно представить в виде группы параметров x распределения потребляемых ресурсов (в соответствии с алгоритмами мониторинга состояния сетевых элементов заданного логического уровня ИТКС), определяющих функциональную аналитическую связь между перечисленными выше группами внешних характеристик $Q = F(\Phi, \Xi, \Omega)$. Такая трактовка функциональных характеристик позволяет, фиксируя любые две группы внешних характеристик (например, в соответствии с внешними требованиями к сенсорному-телекоммуникационному уровню подсистемы мониторинга), по показателям третьей группы (возможно, после свертки в один показатель Q) судить об эффективности процесса мониторинга состояния сетевых элементов и ИТКС в целом на соответствующем уровне. При этом оптимизация распределения ресурса будет заключаться в максимизации выбранного показателя эффективности Q путем поиска соответствующих значений параметров $x \in X = X(\Omega)$.

Данная запись предполагает зависимость допустимого множества значений X от внешних и внутренних ресурсов, что указывает на возможный путь декомпозиции внешних характеристик одних уровней при контроле требуемых значений показателей качества других уровней. Это позволит строить взаимоувязанные иерархические модели. Поскольку функционирование сетевых элементов рассматривается в виде контролируемого процесса, реагирующего на изменения состояния объекта и изменение внешних условий, то необходимо

более детально рассмотреть проблемы мониторинга различных уровней иерархии, позволяющими учесть эти особенность при оптимизации ресурсов подсистемы мониторинга.

Представленные на рис. 2 формы ресурсов на сенсорном, телекоммуникационном и диспетчерском уровнях подсистем мониторинга служат составляющими для формирования ее топологических структур. Исходя из такого, предложенного выше, многоуровневого представления объекта исследования, поставленная задача на моделирование перспективной подсистемы интеллектуального мониторинга состояния ИТКС ОП не может быть решена с помощью известных методов одноуровневой оптимизации, использующих достаточно простые аналитические выражения для целевых функций или вероятностно-параметрические модели процесса контроля с небольшим числом состояний ОК, и требует применения новых интеллектуальных подходов и технологий к исследованию процессов функционирования и мониторинга состояния компонент и элементов ИТКС (сетевых устройств, каналов, маршрутов, путей, подсетей) на основе принципов многоуровневого моделирования, последовательной декомпозиции целей и задач, комплексного оценивания состояния объекта мониторинга и итеративной (многоэтапной) процедуры выработки решений.

Таким образом возникает самостоятельная задача по формированию общей структуры и обобщенной архитектуры перспективной системы сетевого мониторинга, совершенствованию принципов ее внутрисетевой организации и разработке концептуальной модели подсистемы интеллектуального мониторинга состояния ИТКС на основе многоуровневого подхода, в которой задача создания (синтеза) подсистемы мониторинга ИТКС решается как задача распределения ресурсов на втором и третьем уровнях (телекоммуникационном и диспетчерском), учитывая, что первый уровень представлен локальным сервером мониторинга. В части же процессов поддержки и принятия решений данные процедуры должны решаться в рамках АСУС.

Требования к перспективной подсистеме сетевого мониторинга

Современные системы мониторинга, чтобы оставаться востребованными на рынке телекоммуникационных услуг проходят наряду с сетевыми устройствами и технологиями постоянный процесс совершенствования и модернизации. Это в свою очередь влияет на изменение требований к системам мониторинга в сторону их ужесточения. В настоящее время выделяют следующие требования к новым системам мониторинга, внедряемым на ИТКС [11-13]:

– *резервирование*: каждое сетевое устройство должно контролироваться произвольным минимальным количеством серверов, например, превышающим один. Это означает, что серверы мониторинга должны проверять, какие сетевые устройства имеют назначенные серверы мониторинга, и, если их количество ниже минимального (менее двух), самостоятельно принимать решение стать сервером мониторинга для любого из этих устройств;
– *автоматическое распределение*: система автоматически выполняет распределение между сетевыми устройствами и серверами мониторин-

га. При постоянной работе служба должна работать автономно без ручного вмешательства;

– *автоматическая реконфигурация*: система должна иметь возможность автоматически обнаруживать неисправные серверы мониторинга (например, из-за сбоев сети или оборудования) и переназначать сетевые устройства функциональным серверам мониторинга. Этот процесс должен выполняться без ручного вмешательства;
– *репликация данных*: собранные данные должны быть реплицированы и распределены по разным частям системы. В случае разделения сети или деградации БД данные по-прежнему должны быть доступны для извлечения службой мониторинга из других сегментов сети;
– *балансировка нагрузки*: рабочая нагрузка мониторинга должна быть распределена по сети и активным серверам мониторинга, а не концентрироваться на нескольких устройствах.

Сравнение перспективных и существующих систем мониторинга приведено в таблице. 1

Таблица 1 – Сравнение перспективных и существующих подсистем сетевого мониторинга

Перспективные системы мониторинга	Существующие системы мониторинга
Автоматическое назначение: на сервере мониторинга программный компонент назначения запускается без предварительного назначения сетевого устройства. Он назначает себе ряд сетевых устройств для мониторинга в соответствии с настроенной мощностью сервера мониторинга	Контролируемые сетевые устройства вручную назначаются серверам мониторинга администратором сети
Автоматическая реконфигурация: проверка назначенного компонента с настраиваемой определенной периодичностью, текущее сопоставление сервера мониторинга и сетевого устройства, а также реконфигурация назначения в соответствии с текущей ситуацией (например, удалить неотвечающие серверы, увеличить количество серверов мониторинга для сетевых устройств, которые не отслеживаются и пр.)	Автоматическое обновление начального сопоставления сетевых устройств серверу мониторинга отсутствует
Избыточность: каждый программный компонент назначения периодически проверяет, что каждое из сетевых устройств контролируется несколькими серверами (т. е. серверы мониторинга проверяют, какие сетевые устройства имеют меньше мониторов, и самостоятельно решают стать монитором для любого из этих сетевых устройств)	Каждое сетевое устройство контролируется только одним сервером мониторинга
Балансировка нагрузки между серверами мониторинга: решения о самостоятельном назначении учитывают мощность сервера мониторинга в зависимости от конфигурации	Нет специального механизма для достижения балансировки нагрузки между серверами мониторинга
Репликация данных: собранные данные реплицируются на распределенные экземпляры баз данных. В случае разделения сети или оттока серверов мониторинга данные по-прежнему доступны на репликах	Хранение данных мониторинга осуществляется на локальном сервере и теряется в случае сбоя сетевого раздела или сервера

Создание технологических измерительных трактов для передачи ТМИ в перспективной подсистеме мониторинга должна осуществляться с максимальным обеспечением интегрального использования всех видов ресурсов (параметрического, телекоммуникационного, ДПУ), а также унификации программно-аппаратных и аппаратно-программных средств (АПС). При этом моделируемая подсистема мониторинга ИТКС должна обладать следующими *свойствами*:

– интеллектуальностью (гибкостью), когда обеспечивается способность подсистемы мониторинга к развитию, в соответствии с эволюционирующей ИТКС ОП, и приспособлению к существующим ситуациям и предполагаемым действиям;
– комбинированностью (федеративностью), при которой обеспечивается возможность комбинирования подсистемы мониторинга с другими подсистемами ИТКС ОП, и прежде всего, с подсистемой управления функционированием;
– открытостью, когда обеспечивается как переносимость компонентов подсистемы мониторинга, так и возможность совместного функционирования компонентов (например, серверов мониторинга), в том числе функционирующих в составе различных систем;
– управляемостью, с обеспечением возможности для управления, контроля и наблюдения за поведением ресурсов, входящих в состав подсистемы мониторинга;
– интегрируемостью, при обеспечении возможности интеграции различных подсистем и ресурсов в состав целого без необходимости дорогостоящих разработок, что предполагает возможность объединения подсистем с различными архитектурами, ресурсами и поведением;
– модульностью, когда обеспечивается возможность автономной работы отдельных частей подсистемы мониторинга (серверов мониторинга), остающихся взаимосвязанными;
– безопасностью, когда обеспечивается гарантия того, что подсистема мониторинга и обрабатываемая измерительная информация (данные) защищены от несанкционированного воздействия [4, 14].

Применение интеллектуальных технологий для реализации процедуры мониторинга на территориально распределенной ИТКС ОП характеризует расширение таких возможностей подсистем мониторинга как сокращение избыточности ТМИ, а, соответственно, сокращение машинного времени процесса мониторинга, оценивания полученной с первичных преобразователей (датчиков) измерительной информации. При этом техническими решениями в подсистеме мониторинга могут являться реализации: параллельного мониторинга сетевого элемента несколькими серверами мониторинга с последующей репликацией БД серверов мониторинга; снижения объема контролируемых параметров (метрик) без снижения свойств достоверности контроля за счет комплексного использования методов контроля – допускового, функционального, диагностического и профилактического [4, 14].

Для реализации процесса мониторинга территориально распределенной ИТКС в условиях неопределенности ТС ее сетевых элементов, вследствие воз-

действий внутренних и внешних ДФ, необходимо использование существующего технологического базиса, основанного на ряде интеллектуальных технологий [2-4, 8, 10-16]:

– извлечения знаний из различных источников;
– прогнозирования и поддержки принятия решений в реальном масштабе времени;
– планирования или управления целенаправленным поведением сетевых элементов в неструктурированных динамических средах (например, применительно к радиоканалам ДКМ диапазона волн, как среды распространения сигналов с высоким коэффициентом ошибок);
– когнитивного анализа данных;
– мультиагетного управления и диспетчеризации ресурсов в распределенных мобильных системах, а также CALS-технологии, Web-сервисы, Virtualization (виртуализация), Grid Computing (грид-вычисления), Neuro Computing (нейрокомпьютерные вычисления), Autonomic Computing (автономные вычисления или самоуправляемые системы), Mesh-сети (ячеистая топология), Cloud Computing (облачные вычисления), Fog Computing (туманные вычисления), LXI-технологии и др.

Общие принципы организации и функционирования подсистемы интеллектуального мониторинга состояния ИТКС ОП

В настоящее время сетевая инфраструктура – это сложный комплекс программно-аппаратных и аппаратно-программных средств, работающих по технологиям проводного либо беспроводного доступа и использующие оборудование широкого круга производителей. Для решения задач поддержания в постоянной готовности к применению по предназначению и обеспечению эффективной технической эксплуатации указанных АПС такого гетерогенного комплекса сетевого оборудования в целом необходимо применение современной организационно-технической идеологии и подходов к построению системы мониторинга его функциональной безопасности, основанной на использовании перспективных интеллектуальных, информационных, сетевых и измерительных технологий.

Обмен ИИ при реализации процесса мониторинга ТС элементов сети предполагает использование сети технологической связи с каналами телеизмерений-телесигнализации (ТИ-ТС): телеизмерений (ТИ) – в направлении «сервер мониторинга (ДПУ) – сетевой элемент» и телесигнализации (ТС) в направлении «сетевой элемент – сервер мониторинга (ДПУ)». Как правило сеть каналов ТИ-ТС организуется наряду с общими каналами сигнализации (ОКС), использующимися АСУС, наложенными на сеть связи общего пользования. Это предполагает, что при передаче служебной информации телеуправления (ТУ), передается также и ИИ о состоянии объектов мониторинга (критически важных элементов (КВЭ) и сетевых устройств, каналов связи, маршрутов, зон мониторинга, подсетей), позволяющая обеспечить мониторинг и управление элементами ИТКС и системой в целом, осуществить технический контроль и реконфигурацию сети (дистанционное переключение каналов и резервирование элементов

сети при их выходе из строя, ввод новых элементов в сеть при ее наращивании или вывод элементов сети из эксплуатации при деградации сети и т. д.), своевременно обнаружить и устранить неисправности, реализовывать эффективную эксплуатацию ИТКС ОП на основных этапах ее жизненного цикла (ЖЦ) и сохранить высокое качество предоставляемых услуг пользователям.

С учетом этого, основными принципами построения подсистемы мониторинга территориально-распределенной ИТКС ОП можно выделить следующие:

– *принцип эволюционного развития*, представляющий возможность подсистеме мониторинга постоянно соответствовать совершенствующейся (эволюционирующей) сетевой инфраструктуре, на основе ее топологической и пространственно-временной неоднородности;
– *принцип интеллектуализации процессов* мониторинга ТС сетевых элементов, базирующийся на использовании перспективных информационных технологий, развивающихся на стыке искусственного интеллекта и распределенной обработки измерительной информации;
– *принцип гибкости архитектуры* на основе методологии открытых систем предполагает возможность реконфигурации (адаптации) подсистемы мониторинга в условиях дестабилизирующих факторов, и наращивания функций контроля ТС сетевых элементов;
– *принцип распределённости и децентрализации* предполагает, что независимо от того, что ИТКС, как правило, имеет строго иерархическую структуру, ее подсистема мониторинга должна позволять осуществление перераспределения функций центра управления функционированием и периферией в зависимости от текущего состояния всей системы;
– *принцип единства* организационно-технических, алгоритмических и программно-технических решений, направленных на разработку предложений и принятия соответствующих решений в СППР на поддержание и восстановление качества функционирования ОК на основе данных мониторинга ТС сетевых элементов;
– *принцип автоматизации процессов мониторинга*, сбора и обработки телеметрической информации о техническом состоянии ИТКС ОП и ее элементов, а также своевременного отображения результатов мониторинга и оповещения должностных лиц подсистемы мониторинга с целью своевременного принятия оперативных решений по связи.

Таким образом, сформулированные общие принципы организации и функционирования интеллектуальных подсистем мониторинга ИТКС ОП в системном аспекте рассматривают ее с общих позиций, независимо от применяемых технологий. Но основным архитектурным принципом моделирования современных подсистем мониторинга распределенных гетерогенных ИТКС является принцип распределения и децентрализации для повышения устойчивости и надежности подконтрольной сети. Остановимся на нем подробнее.

Механизм децентрализованного распределения успешно обеспечивает установку минимального количества серверов мониторинга на одно контролируемое сетевое устройство, что удовлетворяет заданным системным требованиям. Учитывая, что на распределенной ИТКС обстановка по связи постоянно из-

меняется из-за динамичной смены состояния каналов связи и надежности сетевых элементов для повышения отказоустойчивости подсистемы мониторинга предлагается каждому сетевому элементу сопоставлять несколько серверов мониторинга, находящихся на границах подсетей (сегментов сети). При этом принцип распределенности и децентрализации предполагает размещение на сети нескольких реплик серверов мониторинга.

Проведенный в [13, 17, 18] анализ особенностей развитий современных ИТКС и этапов совершенствования показал экспоненциальный рост их структур, порождаемый увеличением географической распределенности, а также возрастанием уровня разнородности сегментов сети, что в свою очередь накладывает особенности на подходы и методы построения структур их подсистем мониторинга. При этом, большая степень размерности контролируемого пространства, с учетом многоуровневой структуры и гетерогенности ИТКС, совокупности наблюдаемых метрик на сетевых элементах, представляющих из себя большие данные (Big Data, предполагает разработку модели системы, способной учитывать вышеизложенные требования, предъявляемые к перспективным системам мониторинга, основным из которых является *децентрализация инфраструктуры мониторинга* функционального состояния распределенных сетевых ресурсов.

При этом использование принципов гибкости архитектур и децентрализации предполагают автоматическое динамическое перераспределения функций между серверами мониторинга и периферией в зависимости от деградации или восстановления (наращивания) сети обеспечивая каждый из объектов мониторинга минимум двумя серверами мониторинга с автоматическим взятием на мониторинг, снятием с него, а также с последующей репликацией (обновлением) распределенных БД и БЗ, накапливающих и обобщающих опыт идентификации ТС сетевых элементов подсистемой мониторинга в процессе ее обучения.

Объектно-субъектное описание подсистемы мониторинга ИТКС ОП

В процессе моделирования перспективной подсистемы мониторинга ИТКС в работе используем следующие термины, раскрывающий типы объектов и субъектов, сущностей и процессов подсистемы мониторинга, таблица 2.

Проведенный в [13] анализ реализации на уровне систем управления базами данных (СУБД) подсистем мониторинга методов моделирования ИТКС ОП показывает наличие двух основных схем: схемы *объектов управления*, описывающих контролируемые каналы, интерфейсы, сети и схемы *субъекта управления* (конфигурация измерительного агента) [19].

Модель объекта управления. Базовыми объектами CIM (Common Information Model – общая информационная модель), GMPLS (Generalized MultiProtocol Label Switching – протокол и модели IETF для обеспечения функционирования технологии MPLS через гетерогенные сети) в данной модели являются те, состояние которых может быть определено непосредственным сетевым измерением без использования информации о состоянии других объектов.

Современные системы мониторинга такие как OpenNMS, HPOpenView, Nagios оперируют тремя типами базовых сущностей:

Таблица 2 – Типы сущностей, процессов, объектов и субъектов системы мониторинга

Сущности, процессы, объекты, субъекты	Характеристика, описание, физический смысл сущности, процесса, объекта, субъекта системы мониторинга
Основные типы сущностей	
«Интерфейс»	Набор средств, используемых для взаимодействия двух систем. «Interface»– буквально «место соприкосновения» (точечный объект)
«Соединение»	(«Линк») Характеризуется последовательностью точек (точка-точка)
Производные групповые сущности	
«Путь»	Последовательность соединений
«Сеть» (сегмент)	Совокупность интерфейсов, соединений, путей
«Узел»	Совокупность интерфейсов
Основные объекты мониторинга	
«Сетевые элементы»	Устройство, канал, интерфейс, соединение, путь, узел, сеть
Уровни обработки измерительной информации	
Первый уровень «Данные» (Data)	Получают посредством измерения (collect) параметров сетевых элементов и групп элементов
Второй уровень «События» (Events)	Получают после обработки процессами сбора первичных данных и сравнения измерения со значением порога. События характеризуют: классом; временем генерации; адресом, при обращении к которому сгенерировано событие; идентификатором программных компонент, сгенерировавших событие; идентификатором диагностируемого устройства-источника. В процессе обработки событие может передаваться по цепочке субъектов: «устройство» – «агент» – «компонент сбора данных» – «компонент диагностики». Формат события имеет ориентацию на модель протокола SNMP
Третий уровень «Отказы» и «Предупреждения»	Отказы (faults) и предупреждения (alarm) получают в результате логического вывода на множестве событий (events)
Субъекты мониторинга	
«Агент мониторинга»	Программный процесс, связанный с актуализируемой моделью протоколом мониторинга (например, SNMP-агент, NetConf-агент)
Компоненты мониторинга:	Производят операции над сетевыми элементами
«Компонент ситуационного анализа»;	Формирует на основе множеств событий отказы (faults) и предупреждения (alarm)
«Компонент визуализации событий»;	Отображает информацию о состоянии сети и ее сетевых элементов с помощью карт как совокупности взаимосвязанных объектов и символов, обеспечивая графическое и иерархическое представление сети
«Компонент корреляции событий»	Определяет первопричины сетевых проблем, фильтруя поток вторичных сообщений об ошибках, сокращая сроки поиска и устранения отказов, оставляя полезные сообщения о работе сети
Компоненты системы мониторинга	
«Компонент диспетчеризации событий» совмещен с «настраиваемым классификатором событий, отказов и предупреждений»	Процесс-диспетчер событий. Сервисы, подключаемые к диспетчеру событий, строятся по проекциям управления: отказами, конфигурацией, учетом, производительностью, безопасностью (Рекомендация М.3703). Соотносятся к системе мониторинга через «Компонент анализа структуры сети»; «Компонент сбора данных»; «Компоненты тестирования высокоуровневых сервисов»; «Компонент работы с отказами»

– протокольная точка – интерфейс устройства любого уровня модели OSI. Примерами первых являются Ethernet-интерфейсы, IP-протокольные точки, а также высокоуровневые порты почтовых (SMTP, POP3) и HTTP сервисов;
– соединение (точка-точка) – объект, характеризуемый парой протокольных точек. Примером соединений являются IP-хоп (две IP-точки), PPP-соединение (2 протокольные точки);
– узел (устройство) – служит для моделирования как нетелекоммуникационных параметров устройства (буферная оперативная память, такты процессор и др.) так и телекоммуникационных. Характеристики (метрики) указанных объектов получают при помощи внешних измерительных средств (тестеров каналов и соединений), а также встроенных агентов тестирования маршрутов и соединений (например, SNMP или NetFlow-агентами).

На основании базовых формируются производные групповые сущности:
– путь – последовательность соединений. Служит для моделирования IP-маршрутов, MPLS-туннелей, SDH-трактов;
– сеть, сегмент – совокупность интерфейсов, соединений, путей.

В процессе функционирования системы мониторинга взаимодействуют с агентами сетевых устройств, предоставляющих данные о состоянии отдельных компонентов (интерфейсов, каналов, подсетей). Каждый агент в IP-сети, как программный процесс, характеризуется парой (IP-адрес и номер порта). Таким образом, с точки зрения подсистемы сбора данных, сеть управления может быть представлена множеством IP-интерфейсов, которые могут принадлежать различным узлам и сетям. На узлах размещаются агенты управления. На одном IP-интерфейсе может размещаться несколько агентов, предоставляющих информацию о состоянии различных элементов устройства и формируемых каналов.

Субъект управления. В качестве субъекта управления выступает программный агент, обеспечивающий измерение характеристик объектов управления. Тогда обобщенная объектная модель в виде «сущность-связь» будет имеет вид, представленный на рис. 3.

Конфигурация агента управления для разных типов объектов управления может быть различной. Для получения сведений об интерфейсе устройства достаточно сообщить агенту номер интерфейса и протокол управления (например, SNMP или WBEM). В то время как для получения сведений о канале необходимо указать для агента пару идентификаторов интерфейсов, характеризующих точку начала, и точку конца. Таким образом, при конфигурировании системы сбора данных в свою очередь должна учитываться конфигурация объекта управления, что и отражается в модели субъекта управления.

Формирование структуры подсистемы мониторинга ИТКС ОП

Большинство существующих проблем в технической эксплуатации сетевых инфраструктур связаны с недостаточной эффективностью процесса управления, отставанием развития информационно-управляющих систем от потребностей, дезинтеграцией и несогласованностью внедрения сетевых и программ-

№5. 2021
ISSN 2410-9916

ных продуктов, трудностями внедрения современных информационных технологий в практику деятельности подсистемы управления функционированием на всех уровнях. Решение задачи повышения уровня готовности сетевых элементов, мониторинга их ТС, выполнения других мероприятий технической эксплуатации, должно основываться на создании перспективной подсистемы интеллектуального мониторинга. Таким образом, существует необходимость в расширении функций и изменении структуры оперативно-технического уровня управления АСУС ИТКС для реализации функций интеллектуального мониторинга сети, позволяющих осуществлять постоянно (в режиме реального времени или близком к нему) или периодически сбор, систематизацию, анализ и представление информации о ТС сетевых элементов, на основе данных мониторинга.

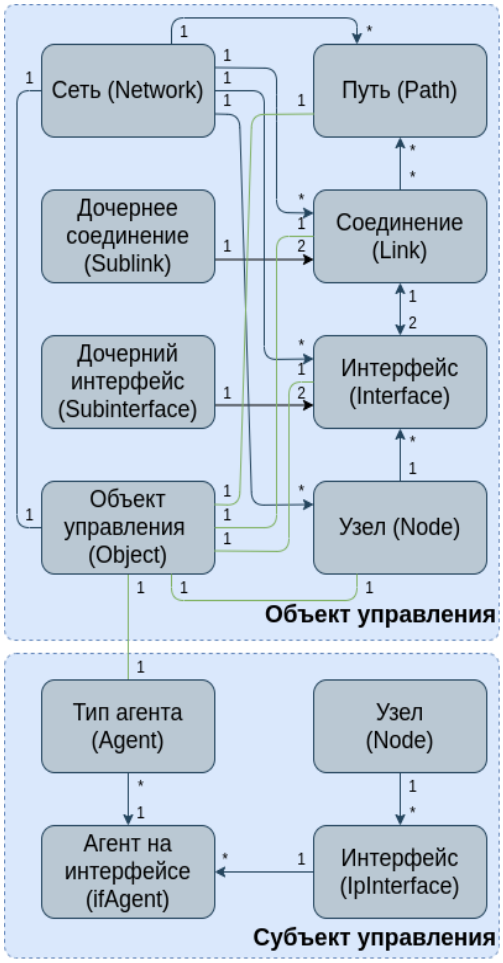

Рис. 3. Субъект-объектная модель подсистемы мониторинга ИТКС ОП типа «Сущность-связь»

Современный уровень развития технологий в области машинного обучения, интеллектуальных агентов, IoT, BigData, CALS-технологий и др., предоставляет расширение возможностей в работе действующих систем сетевого мониторинга, повышает уже имеющуюся степень автоматизации, а также ее интеллектуализации в целом за счет существенного роста эффективности применения каждого отдельного средства контроля, путем использования и объединения всех измерительных ресурсов в единую подсистему. Здесь полностью

DOI: 10.24412/2410-9916-2021-5-65-119
URL: https://sccs.intelgr.com/archive/2021-05/04-Budko.pdf

проявляется *эффект синергизма*, когда целое представляет нечто большее, чем сумма его частей. При этом повышение возможностей подсистемы осуществляется не только за счет улучшения отдельных характеристик средств контроля, а главное за счет информационной связности всех ее компонент [4].

Сегодня процесс, происходящий в развитии измерительных технологий, переходит на качественно новый уровень, характеризующийся [4]: внедрением микропроцессорной техники на уровень первичных преобразователей (сенсоров); использованием технологий открытого взаимодействия, дающих принципиальную возможность получить доступ к диагностической информации, управлению системой из любой ее точки по цифровой шине, по радиоканалу и др., при этом каждый датчик или исполнительный механизм превращается в своеобразный сервер данных (БЗ) и может накапливать и хранить информацию, а также управлять некоторыми контурами управления в системе; реализацией альтернативных алгоритмов измерения и обмена, позволяющих повысить надежность системы; на основе диагностической информации, поступающей от первичных преобразователей, система может прогнозировать изменение характеристик и отказы, как отдельных узлов, так и системы в целом.

Несмотря на сложность организации сенсоров, они приобретают все новые эксплуатационные качества: повышается надежность и точность измерения упрощается обслуживание, снижаются временные затраты на ввод их в эксплуатацию, снижаются эксплуатационные и ремонтные расходы, обеспечивается непрерывная самодиагностика и доступность для контроля, настроек и коррекций непосредственно на объектах мониторинга [4].

Применение новых технологий, типа CALS-технологий (Continuous Acquisition and Life – Cycle Support – информационная поддержка ЖЦ ОК) позволяет существенным образом повысить достоверность, эффективность и др. показатели качества проектируемой подсистемы [20]. Активное внедрение устройств с беспроводным интерфейсом, объединённые в сенсорные сети промышленного и исследовательского назначения, и их миниатюризация, ведут к перспективе появления беспроводных сетей, состоящих из большого числа узлов (до десятков тысяч и более), также способствующих повышению оперативности оценки ТС сетевых элементов.

Технологической основой формирования перспективной подсистемы мониторинга ИТКС ОП является конвергенция современных контрольно-измерительных и информационно-телекоммуникационных технологий, способствующих устойчивому функционированию ИТКС на всех ее организационно-технических уровнях за счет расширения функциональных возможностей контроля и мониторинга в направлениях [4]: постоянного оперативного контроля ТС сетевых элементов в процессе их функционирования (мониторинга), а также периодического по заранее установленной программе (контроллинга); сбора, хранения и анализа информации о ТС сетевых элементов с применением современных информационных сервисно-ориентированных технологий с целью предупреждения возникновения аварийной (предотказной) ситуаций вследствие прогнозируемого увеличения потока отказов; информационной поддержки управления процессом восстановления сетевого оборудования; аудита и

оценки достоверности и объективности сведений о фактическом состоянии ИТКС и ее элементах (подсетей) и пр.

Тенденции внедрения интеллектуальных датчиков, цифровых измерительных приборов (ЦИП) направлены на улучшение метрологических характеристик, расширение функциональных возможностей, повышение надежности, снижение габаритов, массы и стоимости подсистемы мониторинга ИТКС ОП. При решении этих задач целесообразно сокращать действия оператора при повышении достоверности контроля за счет внедрения в подсистемы мониторинга ЭВМ с гибким программным обеспечением (ПО), что должно стать основой синтеза перспективных систем контроля, отличающихся своей универсальностью к возможным изменениям номенклатуры сетевых элементов. Кроме того, результат решения данной задачи является также новым свойством автоматизации и интенсификации процесса контроля ТС, сочетанием гибкости с высоким уровнем достоверности и полноты контроля, которое обеспечивается в основном за счет автоматизации программирования и управления на базе ЭВМ, наделяя эти системы перспективой развития в области искусственного интеллекта [4].

Потребность в создания универсальных систем мониторинга лежит в основе развития интеллектуальных технологий в процессах контроля ТС элементов ИТКС, которые на данный момент, в зависимости от степени сложности синтеза, имеют два пути реализации [4]: создание и внедрение адаптивных (самоорганизующихся) систем; создание систем мониторинга на основе интеллектуальных агентов, многослойных нейросетей, вейвлет-преобразований в процессах оценивания ТС, генетических алгоритмов и др. Следующим этапом развития, предположительно, будут интеллектуальные измерительные системы. При этом их отличительными чертами станут переход от параметрического и функционального контроля к комплексному мониторингу с элементами прогноза ТС. Характерной чертой таких подсистем мониторинга является то, что недостаток априорной информации и неконтролируемый дрейф параметров контроля компенсируется интеллектуальной обработкой ИИ.

Таким образом, применение новых сетевых, информационно-измерительных технологий показывают техническую реализуемость этих подходов по сравнению с устоявшимися стратегиями. А поиск новых методов функционального контроля в режиме реального времени (мониторинга) сводится к тезису, что решение подобной задачи возможно в основном только сетевыми средствами, адаптированными к индивидуальным условиям и целям, чему способствуют эффективные и стремительно развивающиеся технологии [4].

Согласно [21-23], *интеллектуальная измерительная система* (ИИС) – измерительная система, параметры и/или алгоритмы которой в процессе эксплуатации могут изменяться в зависимости от сигналов содержащихся в ней интеллектуальных датчиков. Изменение параметров и/или алгоритмов работы ИИС в процессе эксплуатации осуществляется с целью повышения точности и/или достоверности результатов измерений. ИИС может обеспечивать адаптацию в пределах, установленных в технических условиях, к диапазону и скорости изменения значений измеряемой величины, к воздействию влияющих фак-

торов, включая помехи, к объему выборки, к выбору маршрутов в каналах связи и т. д., а также самодиагностику (самоконтроль), самообучение с целью оптимизации параметров и алгоритмов работы, а в ряде случаев – самовосстановление при возникновении единичного дефекта. При этом под *интеллектуальным датчиком* [22, 23] понимают первичный измерительный преобразователь (или их совокупность), параметры и/или алгоритмы работы которого могут изменяться в зависимости от сигналов, содержащихся в нем преобразователей, также имеющего функцию самообучения. Изменение параметров и/или алгоритмов работы датчика в процессе эксплуатации осуществляется с целью повышения точности и/или достоверности результатов измерений. Интеллектуальный датчик может обеспечивать адаптацию (приспособление) в пределах, установленных в технических условиях, к диапазону и скорости изменения значений измеряемой величины, к воздействию влияющих факторов, включая помехи, а также реализовывать функции самоконтроля и самообучения. В дополнение к сигналам преобразователей, содержащихся в интеллектуальном датчике, параметры и/или алгоритмы его работы в процессе эксплуатации могут изменяться в зависимости от внешних сигналов (например, поступающих со встроенного контроллера).

Системы сетевого мониторинга появились в результате прогресса в области автоматизации, интеллектуализации радиоизмерений и представляют в настоящее время отдельную отрасль техники, как привило, интегрированную (в отличие от средств инструментального контроля) в сетевую инфраструктуру. В связи с увеличением числа модульных конструкций сетевого оборудования, повышением их автономности и усложнением, предусматривается создание контуров управления, решающих отдельные задачи мониторинга ТС в рамках информационно-управляющих систем, что предполагает полную интеграцию всех информационных средств [4].

Характерной чертой современных средств телеметрии, используемых при целевом применении объектов мониторинга, является высокий уровень автоматизации всех процессов получения, передачи и обработки ИИ. Устройства автоматического преобразования, кодирования и обработки ТМИ, построенные с широким применением микропроцессоров, специализированных и универсальных ЭВМ, гарантируют высокую точность и оперативность получения ИИ при числе параметров, измеряемых на одном ОК, доходящем до нескольких тысяч [4].

Основным направлением развития подсистем сетевого мониторинга является программно-аппаратная реализация в виде SCADA-систем, т. е. систем диспетчерского управления и сбора данных, нашедших широкое применение в промышленности, при диспетчерском контроле удаленных магистральных трубопроводов, подстанций и пр. [4].

Специфика функционирования сетевых элементов на ИТКС ОП, заключающаяся в территориальной распределенности ОК, определенной степенью автономности, предполагает проектирование подсистемы мониторинга осуществлять с использованием принципов построения телеметрических систем (ТМС) для реализации процессов сбора, обработки и дистанционной передачи ТМИ на ДПУ (в сервер мониторинга). При функционировании подсистемы мо-

ниторинга на достоверность и своевременность оценки ТС влияет как архитектура сенсорного уровня, так и уровень помех на телекоммуникационном уровне, рис. 2.

Технической основой формирования подсистемы сетевого мониторинга нового поколения является внедрение на всех уровнях управления (АСУС) автоматизированных унифицированных магистрально-модульных и сетевых интеллектуальных измерительных систем единого стандарта, а также виртуальных средств измерений [4]. Это говорит о том, что область применения подсистем мониторинга распространяется не только на контроль и измерение параметров ТС, но и на автоматизированное измерение параметров и вероятностно-временных характеристик (ВВХ) каналов, трактов и сетевых ресурсов с анализом ведомственных телекоммуникационных протоколов.

Анализ тенденций развития современных ТМС и систем сетевого мониторинга показал, что в настоящее время при их построении в распределенном исполнении наряду с активно внедряемым стандартом VXI (применяемым в настоящее время на предприятиях Роскосмоса, Росатома, МЧС и др.) также широко используются комбинации стандартов Ethernet (IEEE 802.3) и Precision Time Protocol (IEEE 1588). Интерфейс LXI разработан для создания автоматизированных измерительных систем, размещаемых, как правило, непосредственно (фиксировано) с ОК в стойках, шкафах или территориально удаленных объектах. При этом физической средой интерфейса LXI являются: медный кабель «витая пара», оптический кабель или их комбинации [4]. Применение технологии LXI целесообразно для объединения отдельных элементов и сегментов (включая построенные на основе магистрально-модульных интеллектуальных систем) при создании территориально распределенных ИТКС, а также для интеграции в нее отдельных интеллектуальных датчиков, сенсоров и т. п. Исходя из чего, создаваемую перспективную подсистему мониторинга ИТКС целесообразно реализовывать на основе распределенной измерительной системы, объединяющей создаваемые проектно-компоновочным способом на основе технических средств VXI локальной сетью, построенной на основе стандартов Ethernet и Precision Time Protocol (IEEE 1588). Использование этой технологии обеспечит возможность масштабирования контрольно-измерительного и диагностического оборудования путем добавления отдельных измерительных модулей в зависимости от решаемых задач, увеличения числа виртуальных средств измерений путем изменения специального ПО (СПО) и добавления новых программных модулей, расширения номенклатуры объектов мониторинга путем разработки оператором дополнительных алгоритмов проверок с помощью встроенного специализированного конструктора алгоритмов и др.

Таким образом, в целях формирования технологической и технической основ построения структуры перспективной подсистемы сетевого мониторинга необходимо разработать следующие основные информационные модули:

– экспресс-контроля ТС сетевых элементов с использованием автоматического (преимущественно) и автоматизированного режима;
– сбора, хранения, актуализации информации о ТС сетевых элементов, качестве телекоммуникационных ресурсов на действующих связях;

– анализа динамики деградационных изменений параметров сетевых элементов и сети в целом;
– репликации и обновления БД (БЗ) по порядку и методам выполнения измерений и операций диагностирования, актуализации библиотеки алгоритмов контроля и диагностирования, в том числе, в формате СПО.

При этом подсистема мониторинга должна обеспечивать:

– информационно-техническое взаимодействие с программно-техническим средствами автоматизации управления объекта мониторинга;
– автоматизированный контроль состояния информационных каналов, маршрутов передачи информации на сети;
– контроль помеховой обстановки в каналах и трактах связи;
– автоматизированное измерение характеристик внешних и внутренних интерфейсов сетевого оборудования на физическом и канальном уровнях;
– сбор, обобщение и анализ данных о ТС элементов сети и его автоматизированном управлении, прогнозирование отказов и коллизий вследствие постепенной деградации параметров и ВВХ информационного обмена;
– автоматическую регистрацию и сбор ИИ в режиме реального времени, с записью результатов на носитель информации для последующего анализа, обработки и хранения результатов оценки ТС сетевого оборудования;
– формирование, хранение и печать отчетов по результатам циклов мониторинга; отображение и оповещение ЛПР при идентификации аномальных состояний ИТКС.

Учитывая существующий задел в части создания инфраструктурных подсистем ИТКС ОП, информационные модули сбора, хранения, актуализации информации о ТС элементов сети должны использовать часть выделенных для этих целей вычислительных ресурсов центров обработки данных (ЦОД), что позволит отказаться от дополнительного парка серверного оборудования и БД, сократить затраты на эксплуатацию, обслуживание и модернизацию подсистемы мониторинга, повысить сохранность и защиту обрабатываемой в подсистеме ДПУ ИИ за счет собственных надежных инструментов и механизмов ЦОД.

Как показано на рис. 2, подсистема мониторинга должна иметь трехуровневую структуру: сенсорный, телекоммуникационный и диспетчерский уровень управления. В связи с чем модели и методы мониторинга разрабатываются в соответствии с этими уровнями. Так на рис 4 отображена структура предлагаемой подсистемы мониторинга на основе обработки накопленных данных и потоковых данных, состоящая из трех методологических модулей: оффлайн-анализа данных, онлайн-анализа данных и поддержки принятия решений, интегрированные в систему.

Важным элементом для проектирования новой подсистемы являются процессы мониторинга, контроля и накопления данных о поведении анализируемой ИТКС ОП. Для обеспечения функционирования предложенной подсистемы могут быть использованы данные мониторинга состояния сетевых элементов и

№5. 2021
ISSN 2410-9916

условий эксплуатации, а также событийные данные об отказах, нагрузках, режимах работы и т. д. Перед сбором данных необходимо определить:

– КВЭ в анализируемых зонах мониторинга (выполняется на основе различных видов анализа, таких как функциональный анализ, дисфункциональный анализ, анализ критичности, накопленный опыт и др.);
– параметры мониторинга сетевых элементов, а также все параметры подлежащие контролю (полный инструментальный контроль);
– интеллектуальные датчики (сенсорный уровень) для отслеживания процесса деградации оборудования.

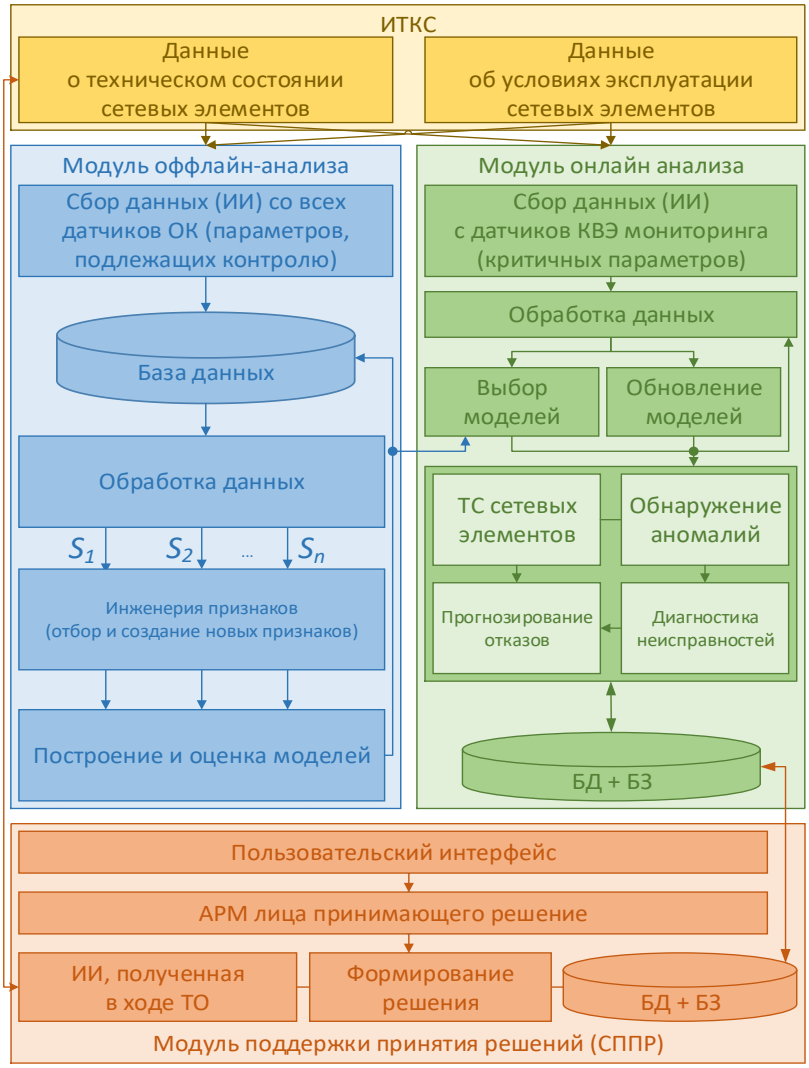

Рис. 4. Предложенная структура процесса сетевого мониторинга

Полученная ИИ должна храниться в БД для последующего анализа.

Модуль оффлайн-анализа данных осуществляет анализ статистически накопленной ИИ, полученной из однотипных систем с использованием различных алгоритмов машинного обучения, глубоких нейронных сетей и технологий инженерии признаков, преобразования ИИ для формирования моделей, позволяющих ранее обнаружение и диагностику неисправностей, прогнозирование остаточного ресурса сетевых элементов и т. д. Эти модели оцениваются и выбираются для последующего использования в модуле онлайн-анализа данных.

DOI: 10.24412/2410-9916-2021-5-65-119
URL: https://sccs.intelgr.com/archive/2021-05/04-Budko.pdf

Для создания прогнозирующих моделей могут быть использованы методы опорных векторов (SVM), деревья решений (CART), случайный лес (RF), экстремальный метод градиентного бустинга (XGBoost), сети долгой краткосрочной памяти (Long short-term memory, LSTM), сверточные нейронные сети (Convolutional Neural Network, CNN) и др. [4]. Кроме того, известны [24] алгоритмы для раннего обнаружения неисправностей в ОК, такие как скрытые марковские модели, модель ARIMA, LSTM-автоэнкодеры и др.

Модуль онлайн-анализа данных осуществляет сбор актуальных на данный временной интервал данных в реальном времени только из КВЭ, выбранных на основе анализа в модуле оффлайн-анализа данных. Выбранные из модуля оффлайн-анализа данных модели используются для определения и прогнозирования состояния сетевых элементов в реальном масштабе времени. Однако эти модели в процессе использования на потоковых данных реального времени могут устареть в силу многих факторов, например возможности возникновения новых типов неисправностей, на которых модели не обучались в прошлом. Поэтому возникает необходимость переобучения и обновления моделей. Модуль онлайн-анализа данных предлагаемой подсистемы мониторинга предусматривает решение этой задачи.

Модуль принятия решений по результатам мониторинга (на уровне ДПУ) основной целью имеет оптимальное планирование воздействий по ТО и ремонту (через органы управления эксплуатацией сетевой инфраструктуры министерств и ведомств). ИИ, полученная в процессе мониторинга и прогнозирования в модуле онлайн-анализа данных, используется для выработки рекомендаций по оптимальному использованию сетевых элементов и сегментов сети в режиме онлайн. В этом модуле предоставляется пользовательский интерфейс, обеспечивающей передачу ИИ между оператором (ЛПР) и программно-аппаратными компонентами системы о результатах процесса анализа (обнаружение/диагностика/прогнозирование), а также визуализации потоковых данных в реальном масштабе времени. На их основе при необходимости формируются оптимальные управления по переконфигурации сети (оперативно-технический уровень управления связью), а в дальнейшем по ТО и ремонту (технологический уровень управления связью).

Исходя из изложенного, структуру подсистемы мониторинга такой распределенной гетерогенной ИТКС можно смоделировать как неполный ориентированный граф $G = (N, E)$, где N – это набор узлов, составляющих сеть, а E – набор связей (беспроводных или оптоволоконных), соединяющих корреспондирующие пары узлов. Изолированные узлы сети (т. е. без связей с другими узлами) отбрасываются. При этом для построения подсистемы мониторинга рассмотрим два типа узлов: серверы мониторинга M ($M \in N$) и сетевые устройства, подлежащие мониторингу D ($D \in N$). Связи характеризуются заданной пропускной способностью V_{ij}, $\forall (i, j) \in E$ и задержкой T_{ij}, $\forall (i, j) \in E$, в то время как каждый i-й узел имеет конкретное качество мониторинга (при рассмотрении мониторинга как услуги) QoS_i, $\forall i \in N$, полученное из реальных измерений на сети. Для развертывания подсистемы мониторинга на сети можно разместить не более $M_{\max} = k$ реплик сервера мониторинга. Сервер мониторинга может

№5. 2021
ISSN 2410-9916

быть развернут в сетевом узле, только если этот узел имеет QoS_i выше минимального порога, $QoS_i > QoS_{min}$ [25]. Ссылка узла будет использоваться, если его полоса пропускания выше или равна заданному порогу. При сопоставлении сетевых устройств и серверов мониторинга учтем следующее ограничения (хотя оно может быть установлено и иным, в зависимости от важности выполнения функций и включения КВЭ в ИТКС):

$$\sum_{i=1}^{M_{\max}} m_i \geq 2\,. \qquad (4)$$

Поскольку основными принципами проектирования подсистемы мониторинга являются *распределение* и *децентрализация* для повышения устойчивости и надежности, то необходимо использовать распределенные структуры БД для поддержки децентрализованной координации серверов мониторинга. С этой целью серверы должны хранить распределенное сопоставление серверов мониторинга и сетевых устройств, которое они используют для динамического взятия (и снятия) устройств на мониторинг. Такое динамическое распределение одновременно должно модифицироваться любым из участвующих серверов для поддержки выполнения условия (4). Чтобы обеспечить это, используем технологию CRDT (Conflict-Free Replicated Data Type), когда типы данных можно реплицировать на много узлов и обновлять параллельно без координации между узлами, а также делегируем синхронизацию и согласованность данных на базовый уровень хранения (БД), который обеспечивает определенные свойства (например, гарантированную конечную согласованность при репликации данных).

Распределенное сопоставление на ИТКС серверов мониторинга и сетевых устройств приведено на рис. 5 и в таблице 3. В данной сетевой инфраструктуре группа маршрутизаторов $D1 – D12$ представляют фактические сетевые устройства, соединенные между собой оптоволоконными либо радиоканалами и образующие ячеистую сеть. Вокруг них показаны сервера мониторинга $M1 – M6$, взаимодействующие друг с другом для обмена информацией (репликации мониторинговой информации) и координации своих действий.

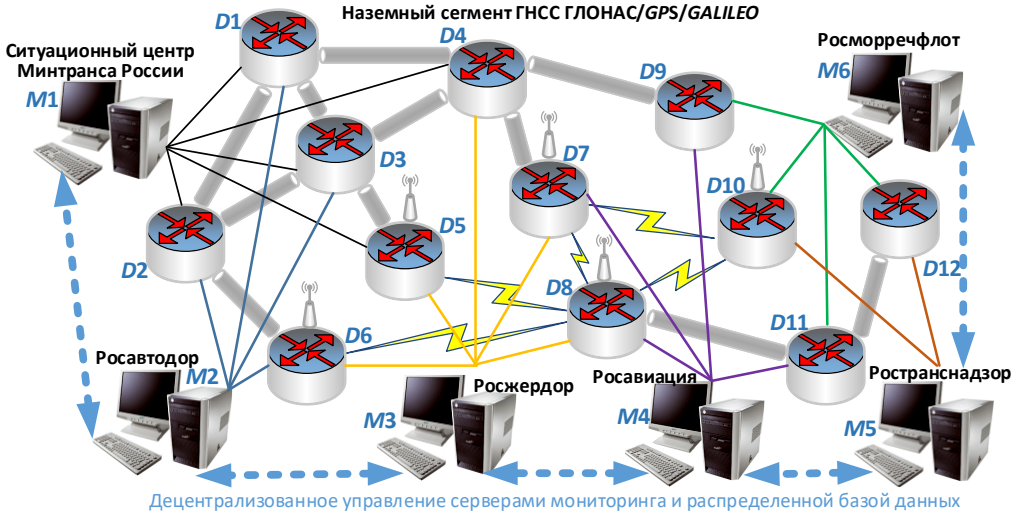

Рис. 5. Децентрализованная подсистема сетевого мониторинга (на примере Минтранса России)

DOI: 10.24412/2410-9916-2021-5-65-119
URL: https://sccs.intelgr.com/archive/2021-05/04-Budko.pdf

Таблица 3 – Сопоставление серверов мониторинга и сетевых устройств (по рис. 5)

Сетевое устройство	Сервер мониторинга	Сетевое устройство	Сервер мониторинга	Сетевое устройство	Сервер мониторинга
*D*1	*M*1, *M*2	*D*5	*M*1, *M*3	*D*9	*M*4, *M*6
*D*2	*M*1, *M*2	*D*6	*M*2, *M*3	*D*10	*M*5, *M*6
*D*3	*M*1, *M*2	*D*7	*M*3, *M*4	*D*11	*M*4, *M*6
*D*4	*M*1, *M*3	*D*8	*M*3, *M*4	*D*12	*M*5, *M*6

Структура, приведенная на рис. 5 может соответствовать межведомственной ИТКС, осуществляющей мониторинг состояния единого дифференциального сервиса Глобальной навигационной спутниковой системы (ГНСС) ГЛОНАС/GPS/GALILEO при его использовании в Министерстве транспорта Российской Федерации в интересах сегментов ИТКС Федеральных Агентств Росавтодора, Росжелдора, Росавиации, Росморречфлота и Ространснадзора для управления движением поездов (ДП), автомобильным транспортом (АПК «Умный город»), систем связи и радиотехнического обеспечения при организации системы управления воздушным движением (ВД), систем автоматизированного управления (АСУ) движением судов (ДС) на внутренних водных путях (ВВП) и в морских акваториях. При этом сервера мониторинга размещаются как на телекоммуникационных структурах автомобильных и железных дорог, районов воздушного движения и районных администраций бассейнов рек (озер), до единых центров управления (ЕЦУ) ДП, ЕЦУ ВД, ЕЦУ ДС и в ситуационном центре (СЦ) Минтранса РФ.

Формирование архитектуры подсистемы мониторинга ИТКС на основе ее функций и реализации функциональной модели управления FCAPS

Информационная архитектура современных систем мониторинга исходит из реализации функциональной модели FCAPS [26], включающую пять основных «функциональных проекций» систем управления и систем мониторинга: управление отказами (Faults); управление конфигурацией (Configuration); управление ресурсами (Accounting); управление производительностью (Performance); управление безопасностью (Security).

В общем случае процесс мониторинга сети включает следующие этапы [27]:

– определение (discovery) структур сети (анализ топологии);
– измерение (collect) параметров сетевых элементов и групп элементов;
– оценка состояния сети с точки зрения возможностей исполнения требуемых функций, а также определение рекомендаций к устранению возникших нарушений в работе.

При первичном развертывании подсистемы мониторинга производится анализ структуры сети (запись в БД информации о топологических отношениях между сетевыми элементами: устройствами, каналами, интерфейсами). На следующих этапах решаются непосредственно задачи управления на основе получаемых в результате измерений первичных данных.

Современные системы мониторинга строятся вокруг концепции события, как агрегированной информации об изменении состояния ИТКС и ее компонентов. Исходя из этого центральным компонентом системы мониторинга яв-

ляется компонент диспетчеризации событий, совмещенный с настраиваемым классификатором событий, отказов и предупреждений (соответственно рекомендаций M.3703 [6]). Сервисы OSS, подключаемые к диспетчеру событий, строятся по проекциям управления: отказами, конфигурацией, учетом, производительностью, безопасностью.

События характеризуются помимо класса, временем генерации, идентификатором устройства-источника (диагностируемого), адресом, при обращении к которому было сгенерировано событие, а также идентификатором программного компонента, его сгенерировавшего. В ходе обработки событие может передаваться по цепочке субъектов «устройство» – «агент» – «компонент сбора данных» – «компонент диагностики» [13, 19], т. е. в процессе обработки событий субъекты выстраиваются в цепочки. Интеграция событий происходит за счет компонента-диспетчера классифицированных событий.

Рассмотрим подробнее работу компонента диспетчеризации [13, 28].

Каждый из компонентов, входящих в систему мониторинга, может быть «подписан» на получение определенного класса событий. В случае возникновения в сети событий, подписчики-обработчики событий извещаются компонентом диспетчеризации. Механизм «подписки» процессов реализуют посредством таблицы «ключ-значение», в которой класс событий выступает в качестве ключа, а список компонентов-подписчиков – в качестве значений.

При поступлении события в компонент диспетчеризации оно обрабатывается цепочкой процессоров:

– процессор для осуществления записи события в БД;
– процессор классификации и расширения описания события. Классификация событий осуществляется за счет подгрузки из классификаторов дополнительных данных;
– процессор рассылки, который на основе таблицы «класс события» – «подписчик» осуществляет широковещательную рассылку события процессам-подписчикам.

Формат события ориентирован на модель протокола управления SNMP. Для выполнения таких измерений достаточно лишь IP-адреса устройства и, соответственно, пароля доступа к нему. Измерение на сети, которая характеризуется группой адресов, или на канале-маршруте, характеризующемся парой адресов, в рассмотренный формат не укладывается и требует расширения. В качестве процессов-подписчиков событий используются компоненты ситуационного анализа, которые на основе множеств событий формируют отказы (faults) и предупреждения (alarms), а также компонент корреляции событий (correlated) и компонент визуализации (отображения).

Механизм корреляции событий определяет первопричину сетевых аномалий, отсеивая огромный поток вторичных сообщений об ошибках. Это значительно сокращает сроки поиска и устранения неисправностей (отказов). Данный механизм автоматически обрабатывает множество второстепенных сообщений, сводя их к нескольким действительно существенным для процесса диагностики, полезным в части характеристики функционального состояния сети.

Для реализации описанного выше принципа интеллектуализации процессов мониторинга ТС сетевых элементов, базирующийся на использовании перспективных информационных технологий, развивающихся на стыке искусственного интеллекта и распределенной обработки измерительной информации, в архитектуру перспективной подсистемы мониторинга включен компонент интеллектуальной обработки ИИ, который должен размещаться между диспетчером событий и компонентом отображения. Поскольку компонент интеллектуальной обработки действует совместно с диспетчером событий, то размещается он также на уровне среды событий, рис. 6. Именно в данном компоненте реализуются интеллектуальные методы обработки ИИ.

Еще одним компонентом – получателем событий является компонент визуализации. В настоящее время системы мониторинга активно используют отображение информации о состоянии сети с помощью символов и карт. При этом карты и суб-карты системы мониторинга относятся между собой как страницы атласа. Подобно атласу, карты, отображаемые системой мониторинга, представляют состояние как всей ИТКС, так и отдельных сегментов данной сети (подсетей). Карта сети, отображаемая на табло системы мониторинга, представляет собой совокупность взаимосвязанных объектов мониторинга, символов и суб-карт, которые обеспечивают иерархическое и графическое представление всей сети связи или отдельных ее частей. Использование карт сетей оправдано при отображении больших, территориально распределенных ИТКС, а также различных способов представления одной сети связи, необходимых оператору для решения конкретной задачи. Схема вычисления состояния задается оператором при помощи правил агрегации и фильтрации событий.

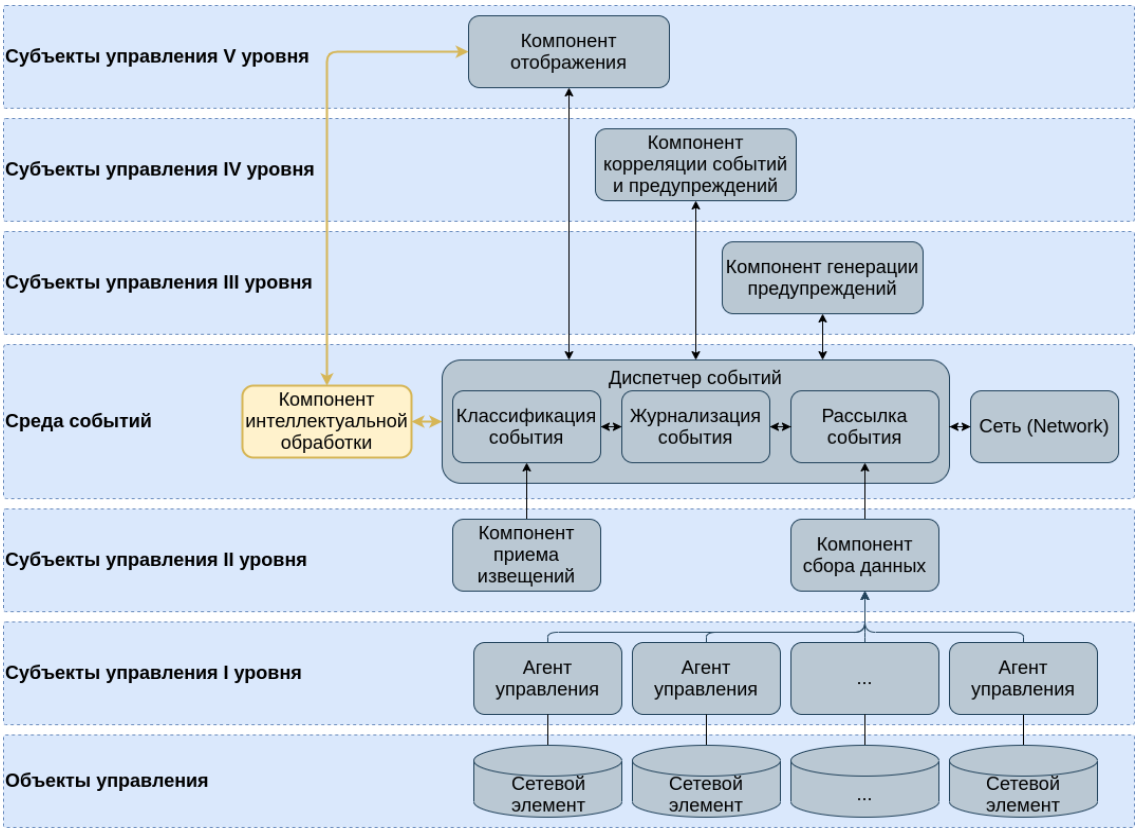

Рис. 6. Общая архитектура перспективной системы мониторинга ИТКС ОП

Таким образом, исходя из сказанного, в окончательном виде среди *основных функций* подсистем мониторинга ИТКС ОП можно выделить следующие:

– *слежение* – основная функция, включающая в себя периодический сбор показателей с узлов оборудования, сервисов и т. п.;
– *хранение информации* (дополнение к слежению). Осуществляется сбор информации по основным показателям каждого объекта мониторинга. Для хранения обычно используются БД;
– *построение отчётов* – осуществляется как на основе текущих данных слежения, так и по долговременно хранимой информации. Например, долговременный мониторинг нагрузки на сервер может предупредить, что потребляемые ресурсы всё время увеличиваются, значит необходимо увеличить доступные средства или перенести часть задач на другой сервер, выбор которого тоже можно осуществить на основе долговременного отчёта;
– *визуализация* – отчёты в визуальном представлении в виде графиков, диаграмм и подсказок способствуют восприятию измерительной информации ЛПР, при этом возможен выбор для визуализации только важных метрик, тогда как в отчётах будут представлены все показатели;
– *поиск «узких мест»* – на основе анализа данных мониторинга возможно узнать, в каком месте инфраструктуры сети наиболее сильно снижаются общие показатели производительности;
– *автоматизация сценариев* – функция освобождает администратора от рутинных задач.

Исходя из проведенного анализа функций подсистем сетевого мониторинга определим основные функции сервера мониторинга перспективной системы мониторинга ИТКС, к основным из которых можно отнести функции выборки, назначения, доступности устройств (ping) и сбора метрик (SNMP):

1. *Функция выборки.* Цель функции выборки на сервере мониторинга состоит в получении последнего (актуального) описания сети и представления его в распределенную базу данных. Программное приложение компонента выборки необходимо запускать во время начальной загрузки подсистемы мониторинга. Его функция – записывать необходимые данные сетевой инфраструктуры в распределенную БД. Впоследствии его можно запускать периодически (например, ежечасно) или по запросу, когда сетевая инфраструктура претерпевает изменения (добавляются новые устройства или оборудование выводится из эксплуатации).
2. *Функция назначения*. Целью данной функции является автоматическое назначение серверу мониторинга сетевых устройств для наблюдения. Программное приложение компонента назначения запускается на каждом сервере мониторинга и в его функционал входит поддержание актуальности сопоставления сетевых устройств серверам мониторинга по мере локального обновления сетевой инфраструктуры. К примеру, если сетевое устройство не контролируется требуемым минимальным количеством серверов, один или несколько из них в итоге начинают наблюдать за доступными (обеспечивающие связность) сетевыми устрой-

ствами (динамически берут их на мониторинг), пока требование обеспечения минимальным числом серверов мониторинга каждого из них не будет выполнено. Это новое назначение немедленно обновляется для совместно используемого объекта распределенных данных и распространяется по всей сети, достигая остальных серверов мониторинга. Назначение между серверами мониторинга и сетевыми устройствами является *динамическим* и со временем меняется, поскольку новые сетевые устройства добавляются в сеть или удаляются из нее по мере того, как балансировка рабочей нагрузки на серверах мониторинга требует переназначения сетевых устройств с одного сервера на другой. При этом важно отметить, что компоненты назначения могут обнаруживать сбой сервера мониторинга, удаляя его из системы и принимая на себя его обязанности по мониторингу. Задача состоит в том, чтобы назначить каждое отдельное сетевое устройство, по крайней мере, как минимум 2 серверам мониторинга. Для этого серверы знают список узлов, за которыми нужно следить, и косвенно координируют друг с другом изменяемый объект данных, заданный соотношением «сетевое устройство ⇔ сервер мониторинга», чтобы выполнить фактический мониторинг всех узлов. Так каждый сервер мониторинга может начать случайный выбор узлов, за которыми еще не ведется наблюдение, и назначить их себе.

3. *Функция проверки доступности устройств* (ping). Целью функции доступности устройств является выполнение проверки связи с сетевыми устройствами, назначенными серверу мониторинга, и запись результатов измерений в БД. Программное приложение, реализующее его, находится на каждом сервере мониторинга и заботится о фактическом зондировании сетевых устройств. ПО периодически проверяет назначенный список сетевых устройств для оценки их быстродействия, времени безотказной работы и расстояния до них (с помощью анализа времени приема-передачи пакетов ping). Собранные данные хранят в одном экземпляре распределенной БД. Их репликация между всеми экземплярами гарантирует, что новые данные автоматически реплицируются и распределяются по всем экземплярам БД, обеспечивая избыточность хранения.
4. *Функция сбора метрик.* Назначение данной функции состоит в выполнении SNMP запросов к сетевым устройствам, которым назначен сервер мониторинга, и запись собранных SNMP значений в БД. Программное приложение, реализующее его, запускается на каждом сервере мониторинга и заботится о фактических SNMP запросах к сетевым устройствам. Все собранные данные хранятся в экземпляре распределенной БД. Опять же, репликация данных между всеми экземплярами гарантирует, что новые данные автоматически реплицируются и распределяются по всем экземплярам базы данных, обеспечивая выполнение технологии CRDT (Conflict-Free Replicated Data Type), когда типы

данных можно реплицировать на много узлов и обновлять параллельно без координации между узлами.

Благодаря наличию средств для реализации всех этих функций администратору ИТКС нет необходимости проверять вручную состояние каждой составляющей системы. При этом возникающие проблемы решаются и отказы устраняются более оперативно, диагностика осуществляется многомерно и точно, возможно планирование расширения инфраструктуры.

Обобщенная схема метасистемы и особенности этапов концептуального моделирования

В общем виде под концептуальной моделью в научном сообществе понимают модель, отражающую с необходимой полнотой систему-прототип, в том или ином содержательном аспекте, и сформулированную на естественном языке с использованием положений логики здравого смысла или теоретико-множественных построений [29]. В других источниках [30] под концептуальной понимают модель, представленную множеством понятий и связей между ними, определяющих смысловую структуру рассматриваемой предметной области или её конкретного объекта. Другими словами, это абстрактная модель, определяющая структуру моделируемой системы, свойства её элементов и причинно-следственные связи, присущие системе и существенные для достижения цели моделирования. В соответствии с [30] концептуальная модель формируется после процесса концептуализации или обобщения.

Таким образом, рассмотрев выше многоуровневый подход к процессу моделирования перспективной подсистемы мониторинга ИТКС ОП, сформировав требования, а также общие принципы организации и функционирования подсистемы сетевого мониторинга, определив ее обобщенную структуру и общую архитектуру, построенную на базе основных функций и реализаций функциональной модели управления FCSPS, перейдем к построению общей модели подсистемы интеллектуального мониторинга состояния ИТКС ОП.

Сформулированная выше задача по моделированию перспективной подсистемы сетевого мониторинга является, по существу, задачей синтеза сложной развивающейся многоуровневой (иерархической) системы, относящейся к классу человеко-машинных (эргатических) систем с автоматизированным управлением. Как известно [31-33], формы проведения исследований таких систем достаточно разнообразны и для их проведения не существует универсального рецепта, даже при изучении свойств технических систем, принадлежащих одному виду, не говоря о межвидовых системах [34]. В то же время системный инженерно-кибернетический подход дает возможность сформулировать положения, ограничения и закономерности, позволяющие целенаправленно выстроить концепцию при решении конкретной научно-технической задачи.

Во-первых, необходимость проведения концептуальных исследований обусловлена важностью описания основных свойств моделируемой системы и вытекает из принципиальной неформализуемости сложных систем. Исходя из теоремы Геделя [32] необходимо отметить, что в рамках некоторой формальной системы невозможно вывести все истинные утверждения инженерно-

кибернетической методологии. Речь идет о выделении исследуемой системы из метасистемы, обосновании ее облика и свойств, определяющих потенциальную эффективность в смысле достижения глобальной цели создания системы.

Поэтому целью создаваемой концептуальной модели [32, 33] является установление общих тенденций развития изучаемого процесса, форм и способов его организации, разработка задач и основополагающих принципов применения сложных технических систем. Такое исследование обычно проводится с позиции метасистемы с высокой степенью обобщения. При этом требуется выбрать рациональный вариант структуры системы, такой, чтобы потенциальная эффективность этой системы в процессе функционирования была по возможности наибольшей. Заканчивается концептуальное исследование обычно формированием рациональных требований к системе на основе оценки эффективности различных вариантов.

При ведении концептуального моделирования важно отметить следующие особенности: во-первых, в соответствии с принципом информационной достаточности формирование модели исследуемого процесса обычно начинают с разработки описания организационно-технической системы в виде набора проектных параметров и ограничений, соответствующего системе, частных целей и граничных условий; во-вторых, целесообразно введение четырех качественно различных методологических уровней анализа систем, представленных на рис. 7.

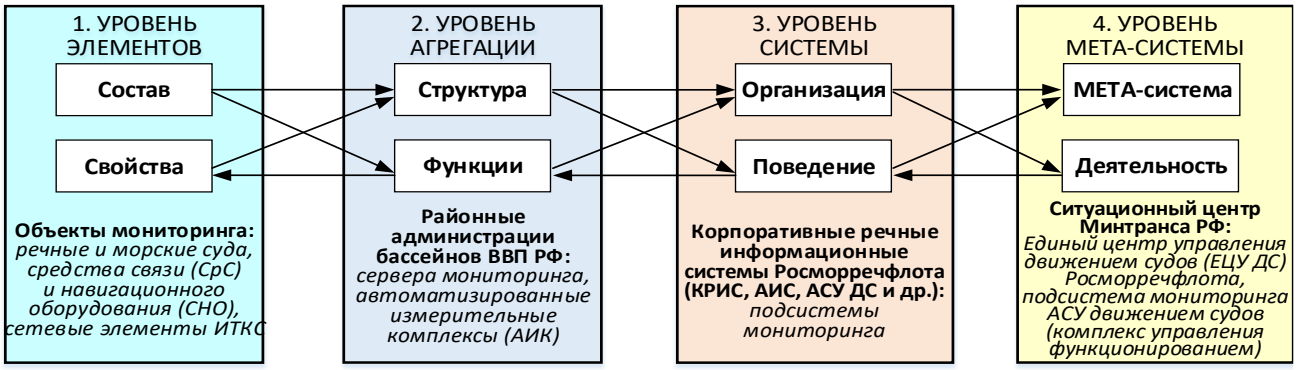

Рис. 7. Уровни анализа ИТКС ОП
(на примере ИТКС Росморречфлота Минтранса РФ)

На рис. 7 на примере ИТКС Росморречфлота Минтранса РФ приведены:

– 1 – уровень элементов, описываемый составом элементов и их свойствами, и охватывающий приемы и методы исследования данных элементов [32]. К элементам первого уровня можно отнести сетевые элементы наблюдаемой ИТКС, морские и речные суда, средства связи и навигационного оборудования, подвергаемые мониторингу. На этом уровне анализируются различные свойства элементов системы, выявляются их эксплуатационные, (надежностные), конструктивные, экономические характеристики и пр.;
– 2 – уровень агрегации, описываемый структурой, в которую объединены элементы с ее функциями [32]. К структурам второго уровня можно от-

нести, к примеру, районные администрации бассейнов ВВП РФ. Здесь объектом исследований являются операции, проводимые в рамках ограниченных по своим масштабам и разнообразию функций S_0-системы, а относительно моделируемой подсистемы мониторинга – процесс сбора ИИ серверами мониторинга (и автоматизированными измерительными комплексами – АИК) с подконтрольного сетевого оборудования (средств связи (СрС) и навигационного оборудования – СНО);

– 3 – уровень системы, описываемый организацией и поведением S_0-системы большего масштаба. Системы данного уровня иногда называют организационно-техническими. Они могу включать в свой состав несколько технических систем [32]. Примером могут служить корпоративные речные информационные системы (КРИС), автоматизированная система управления движением судов (АСУ ДС), автоматизированная идентификационная система (АИС), и др. Данные организационно-технические системы со сложной иерархической структурой, включают в свой состав подсистемы, сложность которых не превышает сложности систем второго уровня исследования. Например, к ним можно отнести подсистемы мониторинга перечисленных систем (КРИС, АИС, АСУ ДС и др.). При этом отношения между подсистемами нестабильны. Интенсивность их актуализации (репликации данных) может изменяться по времени в зависимости от складывающейся обстановки во внешней среде и внутренних режимов функционирования. Системы подобного типа могут быть формализованы лишь при условии четкого определения гипотезы поведения субъектов системы, отражающие преследуемые ими цели. Эффективность поведения таких систем главным образом зависит от соблюдения правил их функционирования, поддержания структур и способов применения. По назначению. Сложность, а порой и невозможность верификации поведения систем, относящихся к данному уровню, повышает роль теоретических, в том числе концептуальных, исследований по обоснованию выдвигаемых гипотез поведения этих эргатических систем, что требует необходимость проведения исследований по возможностям реализации их целевых установок на более высоком методологическом уровне (в мета-системе);

– 4 – уровень мета-системы, на котором исследуются глобальные системы (мета-системы), имеющие в своем составе организационно-технические системы вместе с их внешней средой. Анализ мета-систем и их деятельности возможен только на вербальном (описательном) уровне [32]. Соотносительно с министерствами и ведомствами мета-системой может выступать такая организационно-техническая система (структура) как ситуационный центр, например СЦ Минтранса РФ с входящими в него подсистемами мониторинга ЕЦУ ДС, ЕЦУДП, ЕЦУ ВД, сопрягаемыми с комплексами управления функционированием информационных систем.

Предложенная в [31-34] системная инженерно-кибернетическая методология есть способ реализации системного подхода к исследованию задач управления эффективности эргатических и организационно-технических си-

стем, основой которого является концепция мета-системы. Данная методология является базой исследования системы третьего уровня, которая рассматривается не изолированно, а как неотъемлемая составная часть мета-системы.

Таким образом, применительно к ИТКС Росморречфлота для ее подсистем мониторинга необходимой выходной характеристикой на системном («организация – поведение») уровне является технологическая структура зон мониторинга (зоны навигации, зоны связи, линии связи и пр.). Применительно же к уровню агрегации («структура – функция») такой выходной характеристикой может служить зона действия базовой станции АСУ ДС, зона действия АИС знаков навигационного оборудования, определенных с учетом их эксплуатационных параметров и параметров судовых транспондеров, как объектов мониторинга (КВЭ) на уровне элементов («состав – свойства»).

Общая модель подсистемы мониторинга ИТКС ОП на примере Минтранса РФ

В настоящее время межведомственные ИТКС ОП приобретают все больший охват, территориальную распределенность и пространственно-временную неоднородность, а также постоянно изменяемую топологическую специфику в виде динамичных структур, перестраиваемых в зависимости от режима функционирования сетевого оборудования, варианта его применения, деградационных процессов естественного и искусственного характера.

Анализ этапов развития ИТКС, проведенный в [13, 17, 18] показал экспоненциальный рост их структур, а значит и контролируемого пространства, порождаемый увеличением территориальной распределенности и неоднородности сегментов сети. При этом большая ее степень размерности, с учетом многоуровневой структуры и гетерогенности $\Psi(t)$, совокупности наблюдаемых параметров (метрик), предполагает наличие такой модели системы мониторинга, которая позволит учитывать принципы построения и требования, предъявляемые к ней, что направлено на решение задачи уровня сложности

$$\Psi(t) = \{\Upsilon(t), W(t)\}, \quad (5)$$

где $\Upsilon(t)$ и $W(t)$ – компоненты, характеризующие топологию структуры подсистемы мониторинга и ее функциональные свойства соответственно.

Для редуцирования (сокращения) контролируемого пространства, характеризуемого пространственно-временной и топологической неоднородностью, представим ИТКС развивающейся системой, построенной на основе кластерной технологии, где каждый кластер (сегмент сети) с учетом эволюционного развития и динамичности структуры можно представить совокупностью *зон мониторинга* $Z_v(t)$, разделенных на *критически важные элементы* (КВЭ), масштабируемые на любом этапе развития, рис. 8.

Из изложенного следует, что наблюдаемая ИТКС комплексируется и агрегируется в процессе эволюции в одну систему, что предполагает развитие ее свойства контролируемости:

$$\Upsilon(t) = \{H_v(t), L_d(t)\}, \quad (6)$$

$$H_v(t) = \{Z_v(t), J_p(t)\}, \quad (7)$$

Рис. 8. Гиперграф топологической взаимосвязи зон мониторинга (на примере ИТКС Минтранса)

где $H_v(t)$ – множество вершин гиперграфа (с учетом большой размерности совокупности сетевых элементов, объединенных в кластеры (зоны мониторинга) и их структуры, $v = \overline{1,x}$), представляемых, к примеру, на рис. 8, федеральными агентствами (Росморречфлот, Росавиация, Росавтодор, Росжелдор) и службой Ространснадзора, т. е. $x \leq 5$; $L_d(t)$ – множество дуг гиперграфа, представляемых d-взаимосвязями между сетевыми элементами; $J_p(t)$ – множество дуг гиперграфа, представляемых из p отношений между КВЭ в зонах мониторинга.

На основе изложенного подхода контролируемые неоднородные сетевые элементы представим упорядоченной по значимости совокупностью зон мониторинга, под которыми следует понимать кластеры ИТКС с разной степенью неоднородности, состоящие из КВЭ. При этом КВЭ могут быть как однородными (например, коммутаторы), но образовывать разные, не связанные непосредственно зоны мониторинга, так и разнородными (для Росморречфлота – оборудование связи, контрольно-корректирующие станции дифференциальной навигационной подсистемы, базовые станции автоматической идентификационной системы и пр.), которые образуют непосредственно связанные зоны. При этом КВЭ представляется технологическим ресурсом, состоящим из неоднородных сетевых элементов, отказ которых приводит к тому, что ОК полностью переходит из предотказного в неработоспособное (аварийное) состояние:

$$Z_v(t) = \{K_{vg}(t);\ g = 1, 2, \ldots, m(t), \ldots, l(t)\}, \qquad (8)$$

где $K_{vg}(t)$ – совокупность из g КВЭ, причем m – необходимое и достаточное число КВЭ, а l – общее число КВЭ в процессе ведения мониторинга ИТКС.

Предлагается следующее определение *критически важного элемента* как элемента агрегации сетевых устройств относительно подсистемы мониторинга ИТКС: это отдельные элементы ИТКС на различных уровнях ее разукрупнения, показатели надежности которых в наибольшей степени влияют на показатели надежности всего сетевого кластера (зоны мониторинга). Относительно контролируемого пространства КВЭ представляются сетевыми элементами с «разукрупнением вниз», контрольный опрос «ниже» которых *может быть нецелесообразен*. Тогда в качестве ограничений и допущений в работе предложено: обнаружение и идентификацию аварийных ситуаций в процессе монито-

ринга состояния ИТКС проводить в зонах мониторинга, ограничиваясь КВЭ, обеспечивающим функционирование других элементов, согласно топологии подконтрольного пространства, в пределах рассматриваемых зон мониторинга. Основываясь на результатах анализа функционирования ИТКС, каждый КВЭ имеет свою топологическую структуру. Возможна нумерация КВЭ с учетом принадлежности их к зоне мониторинга, что позволяет помимо редуцирования образовывать счетное контролируемое пространство, функционирующее на разных организационно-технических уровнях.

За счет предложенной на рис. 9 общей структуры подсистемы мониторинга ИТКС, состоящей из определенных зон мониторинга, которые имеют в качестве пограничных элементов КВЭ (центры сопряжения, узлы коммутации, маршрутизаторы и пр.), можно осуществлять мониторинг сети более эффективно. Такое представление контролируемого пространства дает возможность рассматривать концептуальную модель мониторинга для определения соответствия эксплуатационных параметров средств телекоммуникаций установленным требованиям, объединяя концепции измерений, анализа и тестирования.

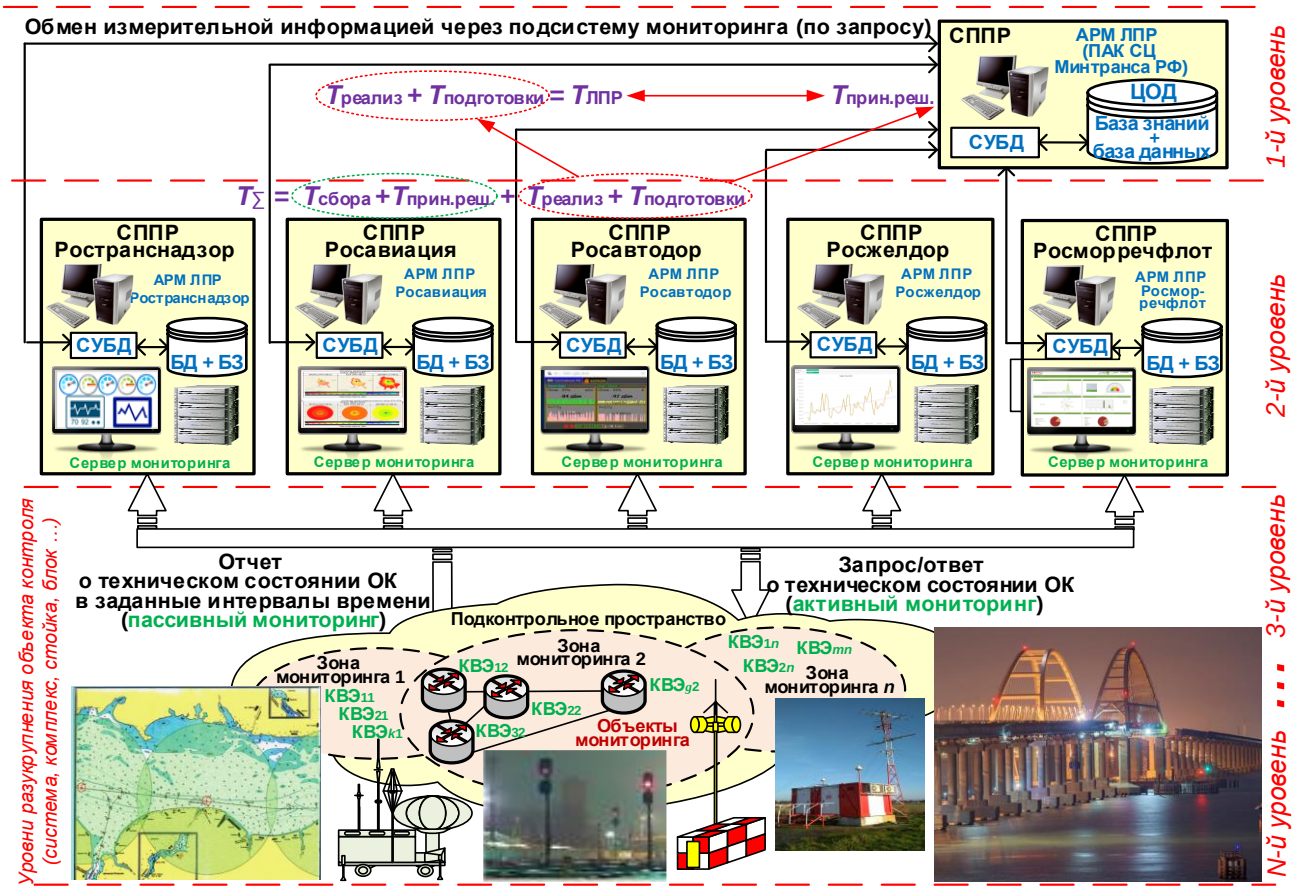

Рис. 9. Многоуровневое представление перспективной подсистемы мониторинга межведомственной ИТКС (на примере ситуационного центра Минтранса РФ)

Особенностью предлагаемого ситуационного управления является процесс передачи ИИ о состоянии КВЭ в зонах мониторинга ИТКС (зона связи, зона навигации, линии связи и пр.) для последующего анализа, что позволит обеспечивать управление системой, ее элементами и осуществлять диагности-

ку, а при необходимости – реконфигурацию ИТКС (дистанционный переход на резерв, переключение каналов, ввод новых элементов в сеть или вывод их из эксплуатации и т. д.). На этой основе возможно своевременное обнаружение и устранение неисправностей – от автоматического процесса сбора ИИ до выработки и принятия решений в СППР ситуационного центра ведомства: в ЕЦУ ДС, ЕЦУ ДП, ЕЦУ ВД, представляющих собой человеко-машинные системы, что повышает оперативность, точность (за счет исключения человеческого фактора) и в целом дает прирост устойчивости ее функционирования.

Для повышения достоверности измерительной информации о ТС КВЭ предлагается расширить количество видов ТС (включая предотказное), классифицируя их до шести [17]. При этом свойства КВЭ в зонах контроля $W(t)$ можно характеризовать квалиметрическими параметрами $B_{kg}(t)$.

Таким образом, расширение числа классов ТС позволит не только осуществлять прогноз состояния ОК, но и более гибко учитывать применение методов их оценки. Такая совокупность предложений позволит на концептуальном уровне редуцировать пространство мониторинга и обеспечивать доставку ИИ до СППР за минимальное время

$$W(t) = \{B_{kg}(t),\ k = 1, 2, \ldots, s(t), \ldots, q(t)\}, \quad (9)$$

где $s(t) = 6$ – необходимое и достаточное число квалиметрических параметров, полученных путем классификации областей работоспособности КВЭ с использованием метода распределенного многоуровневого контроля [35].

На основе результатов мониторинга принимаются управляющие решения по использованию материальных и временных ресурсов для процедуры мониторинга и дальнейшего управления ИТКС. Причем в соответствии с выражением

$$U_{\sum}(t) = R_{\sum}^{v}(t) - R_{g}^{z}(t) \quad (10)$$

управление является функцией времени $U_{\sum}(t)$ в зависимости от суммарного расходуемого ресурса с учетом времени $t_к << t_к^{доп}$, необходимого на проведение контроля сетевых элементов, где $R_{\sum}^{v}(t)$ – суммарный ресурс ОК и подсистемы мониторинга высшего уровня управления (ведомства), $R_{g}^{z}(t)$ – «зональный» ресурс в рамках зоны мониторинга, определяемый числом КВЭ в ней. Очевидно, что ограничение на «зональный» ресурс включает ограничение и на время, расходуемое на контроль ТС элементов сети, расположенных ниже КВЭ. Ограничивая контролируемое пространство до КВЭ приоритетных зон мониторинга, ЛПР получает временной выигрыш на принятие оперативных решений по управлению ИТКС. Данные особенности ОК составляют основу методов интеллектуального контроля, являющихся «нечувствительными» к свойству постоянного эволюционирования (совершенствования) и неоднородности ведомственных и межведомственных ИТКС. Разработка таких методов должна охватывать процессы формирования, оценки и передачи ИИ с целью принятия оперативных решений по результату аварии для обеспечения устойчивого функционирования ИТКС. Исходя из свойств автономности функционирования, топологической и пространственно-временной неоднородности, проявляющихся на гетерогенных ИТКС, процесс контроля их ТС должен осуществляться в режиме реального времени, а их подсистемы мониторинга – проектироваться с учетом адаптации к внешним факторам и внутренним режимам функционирования.

Описание подконтрольного пространства эволюционирующих (изменяющихся) ИТКС и многоуровневая структура телекоммуникационных систем предполагают их разукрупнение в зависимости от степени топологической неоднородности на зоны мониторинга с КВЭ, рис. 8.

Статический и динамический характер функционирования ИТКС на всех уровнях разукрупнения, в зависимости от смены вариантов применения (день/ночь, начало и окончание навигации и пр.) и режимов работы, определяет вариативность ее свойств, характеризуемых протекающими в объектах мониторинга процессами, что выражается в виде пространственно-временной неоднородности. С учетом этого интеллектуальные методы контроля должны обеспечивать выявление зон неоднородности сетевых элементов ИТКС, проявляемых не только топологически, согласно их структуре (по зонам мониторинга и КВЭ), но и по протекающим в них процессам, рис. 10.

Обработка данных (ИИ), поступающих от сетевых элементов ИТКС, подвергаемых мониторингу, осуществляемая на основе систем их распределенной интеллектуальной обработки, поможет реализовать новое интегративное качество, позволяющее спрогнозировать и предупредить негативное развитие процессов согласно определенным законам распределения [13], характеризующим виды ТС (работоспособное, предотказное, неработоспособное и др.) различных критически важных элементов и ИТКС в целом.

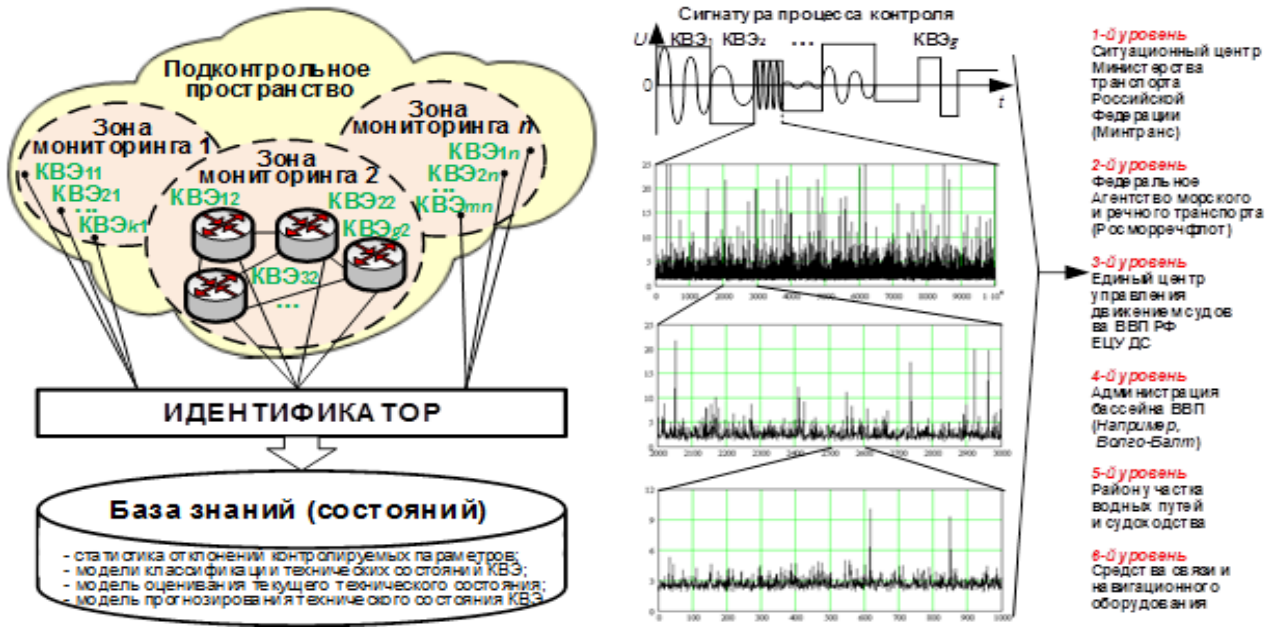

Рис. 10. Структура *m* уровней разукрупнения при агрегации *n* контролируемых процессов (на примере Минтранса РФ)

На основе организационно-технических структур примером уровней разукрупнения, показанных на рис. 10 для Минтранса РФ (*1 уровень*) являются департаменты (агентства и службы) со своими ИТКС (*2 уровень*), ниже идут структуры, определяемые родовыми признаками предназначения, например для Росморречфлота – структуры морского и речного флота в виде ЕЦУ ДС на ВВП РФ (*3 уровень*) с дальнейшим разбиением на администрации бассейнов ВВП РФ

(*4 уровень*), взаимодействующих с ЕЦУ ДС, и далее – на районы водных путей и судоходства (как *низовой уровень*), обеспечивающие эффективное функционирование средств телекоммуникационного и навигационного оборудования ВВП РФ.

Обобщенная модель представления знаний в подсистеме мониторинга ИТКС ОП

В ходе проведения циклов мониторинга состояния ИТКС база знаний (правил) ее подсистемы мониторинга постоянно пополняется новыми данными (ИИ) и реплицируется с другими серверами мониторинга (подсистемами ИТКС) исходя из динамики процесса оценивания ТС сетевых элементов, различных аварийных ситуаций и с учетом условий их протекания. Постоянно пополняемые и обновляемые данные содержатся в правилах и применяются ими в различных аварийных ситуациях для обеспечения выработки решений в управляющей системе (например, в СППР, рис. 9), что обеспечивает гибкость системы контроля.

В результате подсистема мониторинга обеспечивает решение задач: обнаружения, распознавания и идентификации отказов на ИТКС, выделения опасных трендов развития аварийных ситуаций, ведения их оперативного каталога, прогноза отказов, формирования и принятие на основе всестороннего анализа обстановки превентивных мер по обеспечению функциональной безопасности ИТКС, как целевой функции. Актуальным в данном случае является обеспечение решения данных задач в реальном масштабе времени (режиме мягкого реального времени) в автоматическом/автоматизированном режиме функционирования ИТКС.

При этом БЗ моделируется на фундаментальных математических положениях метатеории, как информационная многоуровневая мета-система (рис. 7), способная на основе поступающей ИИ, путем ее обработки получать и применять новые знания в виде правил. Префикс «мета» имеет первоначальный смысл: следовать за чем-либо, переход к чему-либо другому, перемена состояния, трансформация из одного состояния в другое. В современной терминологии префикс «мета» используется для обозначения не только следования, но и обобщения [4]. Метамодель (ММ) БЗ обобщает другие модели, например, обобщенные модели совокупности выборок измерений (временных рядов), результаты уравнивания, модели трендов, полученные на основе выборок эмпирических наблюдений, прогнозные модели о возможном появлении или развитии аварийной ситуации [4].

В моделируемой подсистеме мониторинга ММ БЗ зависит от аварийной, а, соответственно, информационной ситуации. В разных информационных ситуациях ММ имеют разные виды. ММ измерений означает обобщенную модель измерений (методологию), из которой для конкретных условий можно образовать разные конкретные методики измерений. При этом ОК, представляющий собой КВЭ какой-либо зоны мониторинга или аварийную ситуацию, развивающуюся в ней, служит в качестве источника, отражающего происходящие изменения в сетевом элементе территориально распределенной ИТКС. ОК может

порождать разные модели в разные циклы наблюдений на основе общей метамодели наблюдений [4].

Используя положения метатеории, в понятие ОК можно включить систему, явление и процесс. При этом ИТКС и ее подсети с сетевыми элементами (КВЭ) и процессы их мониторинга будем считать эргодическими, так как, эргодичность – специальное свойство динамических систем, состоящее в том, что в процессе развития каждое состояние системы, характеризуемое видом (классом) состояния, с определенной вероятностью проходит вблизи любого другого состояния системы. Основной особенность этих процессов является то, что математическое ожидание (МО) по временным рядам должно совпадать с МО по пространственным рядам. Среднее по времени должно быть равно среднему по статистическому ансамблю. На практике это дает возможность долговременные наблюдения заменять на массовые наблюдения. В обоих случаях получают одинаковые результаты, если система или процесс являются эргодическими.

В пространственном анализе и в теории искусственного интеллекта различных отраслей знаний часто исследуют отдельные объекты, которые в диагностике используют как для основных, так и для вспомогательных целей, трансформируемые в модель информационной ситуации (ИС). Основным объектом исследования процесса мониторинга ИТКС являются пространственные ситуации (аварийные ситуации объекта мониторинга, состояние которого варьируется в пространстве параметров) или информационные пространственные ситуации. При контроле территориально распределенной ИТКС отдельные ОК описываются также моделями ИС, рассматриваемых как ММ в информационном поле. При этом особенностью информационного поля является наличие в качестве элементов поля моделей информационных единиц, которые как элементы алфавита служат основой для построения других моделей [4].

Представление знаний в подсистемах мониторинга включает проведение экспертных оценок, прогнозирование ТС и представление данных результатов для ПОР, что является важным аспектом интеллектуализации процесса мониторинга сетевых элементов на межведомственных ИТКС. При этом процесс прогнозирования состояния объекта мониторинга осуществляется на период, не превышающий время адаптации подсистемы к неоднородности функционирующего элемента (сегмента) сети (включая время ПОР). На примере существующих систем контроля и автоматизированных измерительных комплексов можно заключить, что они достаточно инертны, обладают низким быстродействием и слабо унифицированы, что плохо для охвата мониторингом эволюционирующего сетевого оборудования. При этом, в рамках перспективной подсистемы мониторинга необходим учет данных межведомственных особенностей систем контроля, что определяет необходимость наличия в структуре подсистемы межведомственной БЗ. Применение знаний о КВЭ в межведомственном контролируемом пространстве определяет систему приоритетов и позволяет задать шкалу важности для сетевых устройств (КВЭ), являющейся ситуативной и определяющейся аналогично зонам контроля ЛПР АСУС, поэтому БЗ подсистемы мониторинга должна моделироваться как динамическая, ситуативная и представленная декларативной и процедурной моделями знаний, рис. 11.

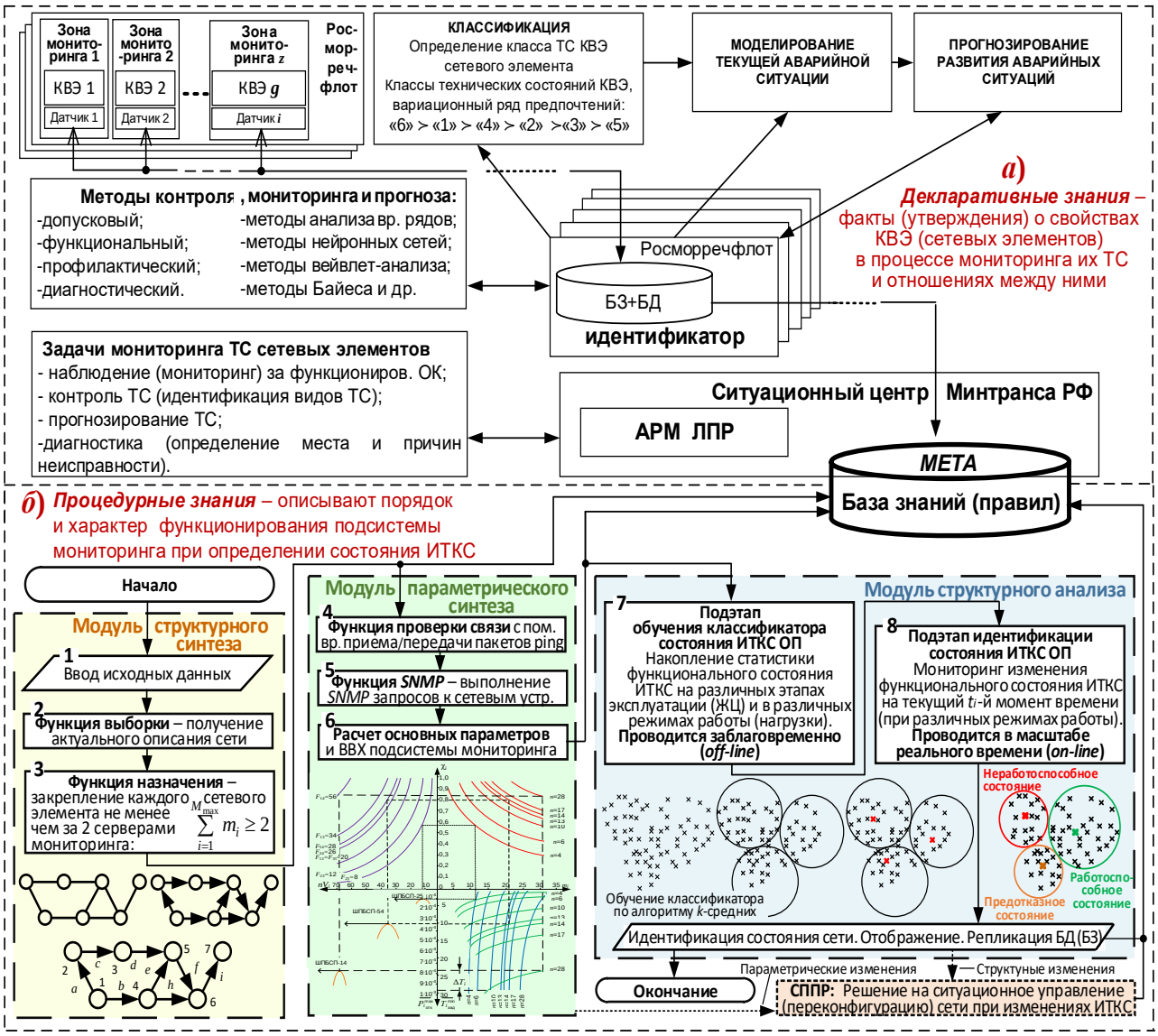

Рис. 11. Обобщенная модель знаний подсистемы сетевого мониторинга

Декларативные знания в БЗ подсистем мониторинга описывают структуру моделируемого объекта исследования (структурные знания), характеризующие процесс мониторинга ИТКС, учитывая межведомственные особенности сетевых элементов, обладающих определенным набором знаний, определяющими специфику, соответствующей министерствам и ведомствам (зон мониторинга Росморречфлота, Росавиации, Росжелдора, Росавтодора, Ространснадзора). Декларативные знания должны описывать совокупность структурных параметров, характеристик ведомственных сетевых элементов, которые определяют структуру процесса мониторинга, с учетом элементов автоматизации АСУС, охватывающих контролируемые КВЭ. Представленная декларативная модель включает процессы сбора и обработки ИИ (временных рядов метрик параметров сетевых элементов). Процедурные знания в БЗ описывают порядок и характер функционирования подсистемы мониторинга при определении ТС КВЭ и состояния ИТКС.

Условия, формируемые на основе поступающей ИИ в БЗ подсистемы мониторинга характеризуют порядок проведения процессов мониторинга ИТКС и

ее элементов, выраженные в следующих *правилах применения методов идентификации* состояния ИТКС:

– основным правилом, определяющим выбор конкретного математического аппарата, в соответствии с БЗ, является степень неоднородности ОК, определяемая по шкале (например, от 0 до 1, в сторону увеличения неоднородности). Наиболее подходящий математический аппарат, в зависимости от степени неоднородности, определяется, например, методом экспертных оценок (в частности, метод бинарных сравнений). В целом обоснование степени важности КВЭ определяется на основе положений теории важности критериев [36]. Для *однотипных КВЭ* (от 0 до 0,6) в процентном отношении от всего объекта мониторинга (подсети), процесс оценивания состояния основана на методах экспертных оценок, метрических методах, методах статистических решений (Неймана-Пирсона, минимакса), статистических методах распознавания, а также искусственных нейронных сетей (ИНС). Это объясняется высокой степенью «схожести» (унификации) сетевых устройств, а также фиксируемым потоком ИИ, характеризуемым свойствами однородности. Процесс изменения функционального состояния в однотипных КВЭ более плавный, что способствует относительно высокой эффективности процессов обучения и обобщения, например, при использовании ИНС. Для *неоднотипных КВЭ* (например, сетевого оборудования), отличающихся импульсным, нестационарным характером потока ИИ с пуассоновским законом распределения или Вейбула («рваный» сигнал, получаемый с большим разбросом) [13], поступающего с подконтрольных КВЭ (при степени неоднородности от 0,7 до 1), наиболее применим метод дискретных вейвлет-преобразований (ДВП), а также метод последовательного анализа Вальда [4];
– для каждой зоны мониторинга имеется своя совокупность правил, зависящих от степени значимости КВЭ. Анализ функционирования телекоммуникационного ресурса ИТКС показал, что наиболее значимыми КВЭ с точки зрения управляемости (контролируемости) являются модемы, коммутаторы, маршрутизаторы, центры сопряжения, а с точки зрения энергетического баланса – силовое оборудование (контроллеры в силовых модулях, энергоблоках и т. д.). С учетом такой интерпретации вводятся три степени значимости КВЭ [4]: к КВЭ первой степени значимости относят коммутаторы и маршрутизаторы и др., к КВЭ второй степени значимости – рабочие станции (ЭВМ) и др.), к КВЭ третьей степени значимости можно отнести электропитающее оборудование, в частности контроллеры силовых модулей, технологическое оборудование обеспечения функционирования сетевых элементов и др. Для критически важных инфраструктур (КВИ) степени значимости КВЭ могут корректироваться;
– процесс оценивания ТС зон мониторинга с КВЭ включается только в том случае, когда число контролируемых КВЭ $m \geq 100$ (определено в результате имитационного моделирования). Причем, как указано в [4], с

увеличением числа КВЭ эффективность мониторинга экспоненциально растет, рис. 12;

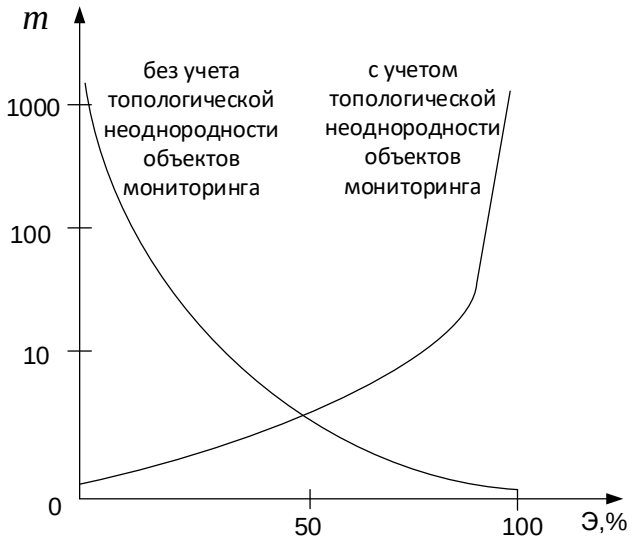

Рис. 12. График зависимости эффективности системы контроля от числа КВЭ [4]

– процесс оценивания зон мониторинга отображается на временной оси с помощью временных рядов [13], а для отдельных КВЭ – в соответствующие интервалы времени (диапазоны, кванты, квазистационарные отрезки времени) [13, 17, 18]. Выделенные стационарные фрагменты (временные «окна контроля») отдельных КВЭ, подвергаемых мониторингу, представляют собой сложный процесс (мультипликативную свертку), состоящий из суммы отдельных наложенных случайных подпроцессов в рамках данного КВЭ. При обработке данных подпроцессов необходимо обращение к БЗ с большим оперативным полем, охватывающим всю систему, за информацией более частного характера (как правило обращение происходит к БЗ более высокого уровня, например – мета-системы, на рис. 10 – это БЗ ситуационного центра ведомства) Такое обращение осуществляется согласно рассматриваемых подпроцессов, в зависимости от их количества, в рамках контролируемого КВЭ различной степени сложности и приоритетности аварийной ситуации (динамики, скорости изменения) и др. С учетом чего имеется возможность в рамках данного КВЭ произвести свертку правил в конечный результат, разработку стэка (абстрактный тип данных, представляющий собой список элементов, организованных по принципу LIFO), позволяющего осуществить сложение отдельных подпроцессов в единый вариационный ряд;
– правило разграничения (распределения) процессов мониторинга, в соответствии с законами распределения, характеризуется количеством зон мониторинга, сложностью и иными особенностями рассматриваемых КВЭ, и определяемых, например: для стационарного характера потока ИИ – нормальный (гауссовский) закон распределения, гамма-

распределение, равномерное распределение; для нестационарного характера потока ИИ – экспоненциальный, Вейбулла, Парето, пуассоновский закон распределения, биномиальное (дискретное) распределение [13]. Таким образом, процесс обработки ИИ основан на работе с *n* числом распределений, равным или меньше числа зон мониторинга, а, соответственно, числа КВЭ. В связи с этим, распределение квазистационарных наблюдаемых процессов на выделенных временных «окнах контроля», осуществляется как распределение распределениями в рамках отдельного интервала времени при контроле КВЭ на *k* уровнях разукрупнения, характеризуемые на начальном, среднем и окончательном интервале этого временного окна [4];

– учет темпа развития аварийной ситуации в наблюдаемых зонах мониторинга влияет на скважность опроса и приоритетность КВЭ [13]. Чем выше скорость изменения метрики, тем выше должен быть приоритет обслуживания КВЭ, а также требуется увеличение скважности опроса, пропорциональное изменению динамики отклонения от нормы значения параметра;
– скорость реакции подсистемы мониторинга на изменение аварийной ситуации зависит от своевременного обновления ИИ, содержащейся в БЗ и используемой в настоящих правилах в соответствии со статусом результата контроля: подтвержденный, нормальный, ориентирующий, экстраполированный и недостоверный. При этом статус «*подтвержденный*» указывает, что результат измерений подтвержден дополнительной информацией о исправности КВЭ или всей зоны мониторинга и риск использования недостоверного результата измерений пренебрежимо мал. Этот статус желателен при ПОР системой АСУС, например при управлении режимами работы и присваивается результату измерений, полученному подсистемой мониторинга от интеллектуального датчика в целом при поступлении информации о исправности КВЭ. Статус «*нормальный*» указывает, что риск использования недостоверного результата измерений невелик, что позволяет, например, принять решение по управлению оборудованием в обычных ситуациях. Статус «*ориентирующий*» указывает, что риск использования недостоверного результата измерений повышен из-за появления дефекта, отказа в КВЭ, но результат измерений может быть применен для ориентировочной оценки состояния сетевого оборудования и хода процесса мониторинга. Данный статус достаточен для принятия решения в случае, например, когда параметры процесса функционирования ИТКС далеки от предельно допустимых. Присвоение результату измерений статуса «ориентирующий» указывает на необходимость выполнения обслуживания КВЭ или измерительной системы и установления сроков этого обслуживания. Статус «*экстраполированный*» указывает, что в качестве результата измерений используется результат, полученный путем экстраполяции данных из предыдущего интервала времени, поскольку поступающая ИИ недостоверна в течение известного интервала времени. Та-

кой статус дает основание, например, для задержки ПОР по управлению ИТКС до появления достоверной ИИ или принятия некоего осторожного решения, ориентируясь на гипотезу, что в течение этого известного интервала времени ТС КВЭ и ход контролируемого процесса функционирования ИТКС не претерпевает заметных изменений. Статус «*недостоверный*» указывает, что риск использования недостоверного результата измерений велик. Следует принять решение об остановке сетевого оборудования или переконфигурации (резервирования) сети. Совокупность статусов «подтвержденный» или «нормальный», а также «ориентирующий» и «недостоверный» соответствует трехзонной системе оценки риска, согласно вероятностного графа состояний [37] объекта мониторинга (аварийное, предаварийное, нормальное);

– для повышения точности, достоверности идентификации (процессов мониторинга и диагностики) вводится адресное пространство КВЭ. За КВЭ закрепляются номера ОК с признаком зоны мониторинга (номер зоны контроля, например, *N*_1.5.2), что позволяет вводить для каждого номера ОК свой набор правил (используя тот или иной метод контроля);
– в чрезвычайных условиях вводится ускоренный алгоритм мониторинга, суть которого сводится к параллельной обработке ИИ, поступающей с КВЭ (однородных и неоднородных), что обуславливает повышение производительности подсистемы мониторинга, причем число потоков зависит от числа различных по неоднородности зон мониторинга. Особенностью подсистемы мониторинга в таких случаях является немедленная реакция на корректировку аварийной ситуации, что определяется *on-line* обновлением ИИ о ТС ОК в БЗ подсистемы мониторинга.

Таким образом, предложенная ММ представления знаний, а также варианты ее применения, является ключевым положением в концептуальной модели подсистемы мониторинга состояния ИТКС ОП, и состоящей из перечня взаимосвязанных понятий, используемых для описания предметной области интеллектуального контроля, совместно со свойствами и характеристиками, классификацией этих понятий по типам, ситуациям, признакам в данной предметной области и законов протекания процессов в ней. Представленная образно-понятийная модель знаний моделируемой подсистемы мониторинга дает оператору (ЛПР) в человеко-машинной системе управления целостную картину и потому обеспечивает возможность соотносить разные части процесса с целым, а, соответственно, и действовать эффективно, тем самым обеспечивая устойчивое функционирование территориально распределенной ИТКС ОП.

Заключение

Таким образом, Проведенный анализ этапов развития сетевых инфраструктур показал непрерывный, экспоненциальный рост контролируемого пространства, порождаемый увеличением территориальной распределенности и неоднородности межведомственных ИТКС в процессе их функционирования, что предполагает соответствующий охват средствами мониторинга контроли-

руемого пространства. Для снижения размерности (редуцирования) контролируемого пространства, характеризуемого топологической и пространственно-временной неоднородностью, показано, что любая ИТКС, с учетом свойств эволюционного развития и динамичности изменения структур может быть представлена совокупностью зон мониторинга, разделенных на КВЭ, масштабируемые на любом этапе развития (или деградации) сети. Редуцирование мониторингового пространства дает возможность рассматривать концептуальную модель подсистемы интеллектуального мониторинга состояния ИТКС ОП для нахождения соответствия эксплуатационных параметров сетевых элементов (устройств, каналов, маршрутов, подсетей) установленным требованиям, объединяющей концепции измерений, анализа и тестирования, что позволит обеспечить управление ИТКС и ее элементами, а также реконфигурацию сети, своевременно обнаруживать и устранять неисправности, и, в целом, способствует обеспечению устойчивого ее функционирования.

Формализация контролируемого пространства терминами «зона мониторинга», «критически-важный элемента» и «классы состояния» составляют основу новых методов интеллектуального контроля, являющихся «нечувствительными» к свойству постоянного совершенствования (эволюционирования) и неоднородности межведомственных ИТКС. Функционирование подсистемы мониторинга ИТКС основано на обращении к базе правил (БЗ), накапливаемых в процессе ее эксплуатации, относительно работы которой нет ограничений как по масштабу территориальной распределенности сетевых элементов, так и по их неоднородности, и основанной на когнитивных методах. Пополняемая, обновляемая и аккумулирующая в себе опыт эксплуатации и процессов мониторинга функционирования ИТКС БЗ позволяет провести более быструю оценку (идентификацию) вида (класса) ее состояния и сконцентрироваться там, где выявлено наиболее уязвимое, разрушающее, деструктивное воздействие и, как следствие, наиболее вероятен отказ КВЭ, за счет анализа уровней разукрупнения. Определение степени аварийных состояний контролируемых сетевых элементов осуществляет идентификатор подсистемы мониторинга, анализ которых осуществляется за счет выбора соответствующего метода мониторинга (контроля) при обращении в БЗ.

На основе системного анализа процессов мониторинга состояния территориально-распределенной ИТКС ОП сформулированы общие принципы функционирования перспективной подсистемы мониторинга, определяющие сенсорный, телекоммуникационный и диспетчерский уровни ее построения в системном аспекте, независимо от применяемых технологий, что позволяет упростить ее моделирование. Также на основе технических и технологических основ интеллектуального мониторинга территориально распределенных ИТКС сформирована структура перспективной подсистемы мониторинга, включающая модули онлайн-анализа, оффлайн-анализа и модуля поддержки и принятия решений, распределенных на сенсорном, телекоммуникационном и диспетчерском уровнях, а также общая ее архитектура с компонентом интеллектуальной обработки ИИ в качестве отличительного признака.

Знания в проектируемой подсистеме мониторинга основаны на фундаментальных положениях метатеории, причем БЗ представляет собой информационную многоуровневую метасистему, моделируемую динамической, ситуативной и представленной декларативной и процедурной моделями знаний, а также способной на основе поступающей информации, путем ее обработки получать и применять новые знания в виде правил. Представленная обобщенная модель знаний подсистемы мониторинга дает оператору в человеко-машинной системе управления целостную картину и обеспечивает возможность соотносить разные части процесса с целым, а, соответственно, и действовать эффективно, тем самым обеспечивая устойчивое функционирование территориально распределенной ИТКС ОП.

Исходя из описанного выше многоуровневого подхода к моделированию сетевых инфраструктур и их систем контроля, выбраны показатели эффективности функционирования перспективной подсистемы мониторинга ИТКС ОП, таблица 5.

Таблица 5 – Взаимосвязь показателей системы мониторинга с показателями ИТКС

Уровни подсистемы (ИТКС)	Показатели качества	Параметры системы	Параметры среды	Математическая модель	Ограничения	Функционал оптимизации	Корректировка
Сенсорный (Физический уровень ЭМВОС)	$D = \{\alpha, \beta\}$, $P_{\text{бр сет.эл.}}$, $p_{\text{ош}}$	n – число датчиков, Θ – диапазон профил. доп.	$P_{\text{п}}$ – уров. ДФ $\Theta(\chi) = f(g)$ $\Theta \in \Omega_\Theta$ g – внутр. ДФ	Достоверность мониторинга: $D = \frac{P_{\text{бр}}(t) - \alpha}{P_{\text{бр}}(t) - \alpha + \beta}$	$D \geq D_{\text{треб}}$ $\Theta_{\max} \geq \Theta \geq \Theta_{\min}$	$\alpha \to \min$, $\beta \to \min$, $T_{\text{цм}} \to \min$	Перераспред. параметрич. ресурсов (ресурс физ.ур.)
Телекоммуникационный (Канальный, сетевой, транспортный)	$P_{\text{св}}$ – вероятность связи в каналах ТИ-ТС	K – число каналов, маршрутов ТИ-ТС, $p_{\text{ош}}$, $T_{\text{зад}}$	$P_{\text{п}}$ – уровень помех (ДФ), $\Xi(\chi) = f(g, \lambda)$, $\Xi \in \Omega_\Xi$ λ – внешн. ДФ	Надежность связи: $P_{\text{св}} = f(p_{\text{ош}} \leq p_{\text{ош.доп}})$, переменная структура сети $S = f(T_{\text{цм}}, K, n)$	$T_{\text{цм}} \leq T_{\text{цм.треб}}$	$P_{\text{св}} \to \max$, $S \to \max$	Распределен. аппаратного и канального ресурсов (ресурс ОКС)
Диспетчерский (Сеансовый, представления, прикладной)	$T_{\text{цм}}$ – время цикла мониторинга	$\Upsilon(t) = \{H_v(t), L_d(t)\}$ $P_{\text{ТИ-ТС}} = \|\|P_{ij}\|\|$	Допустимые динамически структуры: $S(\chi) = \Phi\{f(g,\lambda)S\}$ $S \in \Omega_S$	$\chi_{i\,\text{пр}}^{\text{opt}} = f(m_i, n_i)$ – приемлемый набор параметров сети ТИ-ТС для классов сост.ИТКС	$d(\hat{g}_1, \hat{g}_2) < h$, $\sum_{i=1}^{M_{\max}} m_i \geq 2$	Классы сост. $P_{\text{отк}} \to \min$, $P_{\text{норм.ф.}} \to \max$, $\bar{g} = \min_{g \in U} \sum_{i=1}^{n} d\ g, g_i$	Перераспред. параметров ДПУ (структурный ресурс)

Рассматривая данную подсистему, включенную в территориально распределенной ИТКС ОП как в метамодель более высокого уровня, в работе предложено рассматривать моделируемую структуру на трех уровнях, таблица 5:

– на сенсорном уровне, где моделируемую подсистему соотносят физическому уровню ИТКС в соответствие с моделью ЭМВОС (OSI). Показателями качества на этом уровне являются достоверность процедуры мониторинга $D(\alpha, \beta)$, оперативность цикла мониторинга $T_{\text{цм}}$ и вероятность безотказной работы $P_{\text{бр}}$ сетевого оборудования;
– телекоммуникационном уровне, которому ставят в соответствие канальный, сетевой и транспортный уровни OSI, а показателем качества выделяют вероятность связи в канале ТИ-ТС;
– диспетчерском уровне, где подсистеме сопоставляют сеансовый уровень, а также уровни представления и приложений модели OSI. Здесь показателем качества являются оперативность процедуры мониторинга

при идентификации класса состояния ИТКС в ходе сравнения текущих значений метрик подконтрольных параметров с приемлемыми наборами параметров сети ТИ-ТС, соответствующих тому или иному классу работоспособности.

Исходя из вышеизложенного под интеллектуальным мониторингом можно называть такую стратегию, которая всякую пару $\Phi = \Phi(G, S)$ приводит к цели – правильной идентификации состояния ИТКС и ее элементов при решении оптимизационных задач (1) – (3), где критерий качества функционирования подсистемы мониторинга задан в виде функционала:

$$\Phi = \Phi\{G(\Theta, \Xi), S\}.$$

Таким образом, представленные в работе совокупность требований и общих принципов функционирования перспективной подсистемы мониторинга, ее структуры, в терминах технических и технологических основ построения, а также общей архитектуры, сформированной на базе основных функций и реализации функциональной модели управления *FCAPS*, общей модели подсистемы сетевого мониторинга и ее обобщенной модели представления знаний можно рассматривать как концептуальную модель подсистемы интеллектуального мониторинга состояния ИТКС ОП.

Литература

1. Федеральный закон от 07.07.2003 № 126-ФЗ (в редакции от 09.03.2021) «О связи».

2. Буренин А. Н., Легков К. Е. Системный подход к формированию структуры подсистем мониторинга автоматизированных систем управления инфокоммуникациями // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 8. С. 46-50.

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

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

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

6. 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).

7. Report to the Nations on Occupational Fraud and Abuse. URL: https://www.acfe.com/rttn/docs/ 2014-report-to-nations.pdf (дата обращения: 30.07.2021).

8. 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.

9. Раннев Г. Г. Методы и средства измерений: Учебник для вузов. – М.: Издательский центр «Академия», 2003. – 336 с.

10. Срагович В. Г. Адаптивное управление. М.: Наука. Физматлит. 1981. 384 с.

11. Centelles R., Selimi M., Freitag F., Navarro L. REDEMON: Resilient Decentralized Monitoring System for Edge Infrastructures. Conference proceedings. 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), Melbourne, Australia 2020, pp. 91-100.

12. Tangari G., Tuncer D., Charalambides M., Pavlou G. Decentralized Monitoring for Large-Scale Software-Defined Networks. IFIP/IEEE Symposium on Integrated Network and Service Management (IM). Department of Electronic and Electrical Engineering, University College London, 2017, UK. doi:10.23919/INM.2017.7987291 (дата обращения 03.07.2021).

13. Аллакин В. В., Будко Н. П., Васильев Н. В. Общий подход к построению перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей // Системы управления, связи и безопасности. 2021. № 4. С. 125-227. DOI: 10.24412/2410-9916-2021-4-125-227.

14. Охтилев М. Ю., Соколов Б. В., Юсупов Р. М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. – М.: Наука, 2006. – 410 с.

15. Виноградeнко А. М., Будко Н. П. Адаптивный контроль технического состояния сложных технических объектов на основе интеллектуальных технологий // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 1. С. 25-35. DOI: 10.36724/2072-8735-2020-14-1-25-35.

16. Виноградeнко 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.

17. 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.

18. Будко Н. П. Общие принципы функционирования и требования к построению структур перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей // Техника средств связи. 2021. № 2 (154). С. 38-60.

19. Васильев Н. В., Раков И. В., Забродин О. В., Куликов Д. В. Аналитические и синтетические OSS: анализ подходов и методов // Техника средств связи. 2019. № 1 (145). С. 82-94.

20. Дмитриев А. К., Юсупов Р. М. Идентификация и техническая диагностика. – М.: МО СССР, 1987. – 521 с.

21. ГОСТ 20911-89 Техническая диагностика. Термины и определения. – М.: Союзинформ, 1989. – 10 с.

22. ГОСТ Р 8.673-2009 Датчики интеллектуальные и системы измерительные интеллектуальные. Основные термины и определения. – М.: Стандартинформ, 2009. – 13 с.

23. ГОСТ Р 8.734-2011 Датчики интеллектуальные и системы измерительные интеллектуальные. Методы метрологического самоконтроля. – М.: Стандартинформ, 2011. – 14 с.

24. Рыжиков Ю. И. Теория очередей и управление запасами. – СПб.: Питер, 2001. – 384 с.

25. Вичугова А. Как измерить эксплуатационную надежность Big Data и зачем это нужно – URL: https://www.bigdataschool.ru/blog/sre-indicators-devops-itil.html (дата обращения 21.07.2021).

26. 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).

27. Бломмерс Дж. OpenView Network Node Manager: Разработка и реализация корпоративного решения. – М.: Интернет Университет Информационных Технологий, 2005. – 264 с.

28. Зителло Т., Вильямс Д., Вебер П. HP OpenView – настольная книга системного администратора. – М.: ЭКОМ, 2006. – 616 с.

29. Макаренко С. И. Справочник научных терминов и обозначений. – СПб.: Наукоемкие технологии, 2019. – 254 с.

30. Tatomir A., McDermott C., Bensabat J., Class H., Edlmann K. Conceptual model development using a generic Features, Events, and Processes (FEP) database for assessing the potential impact of hydraulic fracturing on groundwater aquifers. Advances in Geosciences. Copernicus GmbH, 2018, vol. 45, pp. 185–192. doi: 10.5194/adgeo-45-185-2018.

31. Левин В. И. Структурно-логические методы исследования сложных систем. – М.: Наука, 1987. – 303 с.

32. Авдуевский В. С. Надежность и эффективность в технике. Справочник в 10-ти томах. Т. 2 «Математические методы в теории надежности и эффективности». – М.: Машиносроение, 1988. – 280 с.

33. Авдуевский В. С. Надежность и эффективность в технике. Справочник в 10-ти томах. Т. 3 «Эффективность технических систем». – М.: Машиностроение, 1988. – 328 с.

34. Рудых С. В. Системы мониторинга и управления судами технического и вспомогательного флота на внутренних водных путях России. Дис. … доктора техн. наук: 05.13.06. – СПб.: Государственный университет морского и речного флота имени адмирала С.О. Макарова, 2013. – 308 с.

35. Будко Н. П., Будко П. А., Виноградeнко А. М., Дорошенко Г. П., Рожнов А. В., Минеев В. В., Мухин А. В. Способ распределенного контроля и адаптивного управления многоуровневой системой и устройство для его осуществления // Патент на изобретение RU 2450447 C1, опубл. 10.05.2012, бюл. № 13. 30 с.

36. Понтрягин Л. С., Болтянский В. Г., Понтрягин Л. С., Гамкрелидзе Р. В., Мищенко Е. Ф. Математическая теория оптимальных процессов. – М.: Наука. Физматлит, 1983. – 392 с.

37. 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.

References

1. The Federal Law of the Russian Federation of July 07, 2003. No. 126-FZ "About communication" (in Russian).

2. Burenin A.N., Legkov K.E. A systematic approach to structure formation subsystems monitoring of automated control systems for the infocommunication. *T-Comm*, 2016, vol. 10, no. 8, pp. 46-50. (in Russian).

3. 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).

4. 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).

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

6. 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).

7. Report to the Nations on Occupational Fraud and Abuse. Available at: https://www.acfe.com/rttn/docs/ 2014-report-to-nations.pdf (accessed 30 July 2021).

8. 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).

9. Rannev G. G. *Metody i sredstva izmerenij* [Methods and means of measurement]. Moscow, Publishing center "Academy", 2003. 336 p. (in Russian).

10. Sragovich V. G. *Adaptivnoe upravlenie* [Adaptive management]. Moscow, Nauka, Fizmatlit Publ., 1981. 384 p. (in Russian).

11. Centelles R., Selimi M., Freitag F., Navarro L. REDEMON: Resilient Decentralized Monitoring System for Edge Infrastructures. *Conference proceedings 2020. 20th IEEE/ACM International Symposium on Cluster. Cloud and Internet Computing (CCGRID)*, Melbourne, Australia, 2020, pp. 91-100.

12. Tangari G., Tuncer D., Charalambides M., Pavlou G. Decentralized Monitoring for Large-Scale Software-Defined Networks. *IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. Department of Electronic and Electrical Engineering, University College London, 2017, UK. doi: 10.23919/INM.2017.7987291 (accessed 30 July 2021).

13. Allakin V. V., Budko N. P., Vasiliev N. V. A general approach to the construction of advanced monitoring systems for distributed information and telecommunications networks. *Systems of Control, Communication and Security*, 2021, no. 4, pp. 125-227. DOI: 10.24412/2410-9916-2021-4-125-227 (in Russian).

14. Okhtilev M. Yu., Sokolov B. V., Yusupov R. M. *Intellektual'nye tekhnologii monitoringa i upravleniya strukturnoj dinamikoj slozhnyh tekhnicheskih ob"ektov* [Intelligent technologies for monitoring and controlling the structural dynamics of complex technical objects]. Moscow, Nauka Pabl., 2006. 410 p. (in Russian).

15. Vinogradenko A. M., Budko N. P. Adaptive control of technical condition of autonomous complex technical objects on the basis of intelligent technologies. *T-Comm*, 2020, vol. 14, no.1, pp. 25-35. Doi: 10.36724/2072-8735-2020-14-1-25-35 (in Russian).

16. 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).

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. Budko N. P. General principles of functioning and requirements for the construction of structures of promising monitoring systems for distributed information and telecommunications networks. *Means of Communication Equipment*, 2021, no. 2 (154), pp. 38-60 (in Russian).

19. Vasilyev N. V., Rakov I. V. Zabrodin O. V., Kulikov D. V. Analiticheskie i sinteticheskie OSS: analiz podhodov i metodov [Analytical and synthetic OSS: review of approaches and methods]. *Means of Communication Equipment*, 2019, no. 1 (145), pp. 82-94 (in Russian).

20. Dmitriev A. K. Yusupov R. M. *Identifikaciya i tekhnicheskaya diagnostika* [Identification and technical diagnostics]. Moscow, Ministry of Defense of the USSR Publ., 1987. 521 p. (in Russian).

21. GOST 20911-89 *Tekhnicheskaya diagnostika. Terminy i opredeleniya* [Technical diagnostics. Terms and definitions]. Moscow, Standartinform Publ., 1989. 10 p. (in Russian).

22. GOST R 8.673-2009 *Datchiki intellektual'nye i sistemy izmeritel'nye intellektual'nye. Osnovnye terminy i opredeleniya* [Intelligent sensors and intelligent measuring systems. Basic terms and definitions]. Moscow, Standartinform Publ., 2009. 13 p. (in Russian).

23. GOST R 8.734-2011 *Datchiki intellektual'nye i sistemy izmeritel'nye intellektual'nye. Metody metrologicheskogo samokontrolya* [Intelligent sensors and intelligent measuring systems. Methods of metrological self-control]. Moscow, Standartinform Publ., 2011. 14 p. (in Russian).

24. Ryzhikov Yu. I. *Teoriya ocheredej i upravlenie zapasami* [Theory of queues and inventory management]. St. Petersburg, Peter Publ., 2001. 384 p. (in Russian).

25. Vichugova A. *Kak izmerit' ekspluatacionnuyu nadezhnost' Big Data i zachem eto nuzhno* [How to measure the reliability of Big Data and why is the]. Available at: https://www.bigdataschool.ru/blog/sre-indicators-devops-itil.html (accessed 21 July 2021) (in Russian).

26. 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).

27. Blommers J. *OpenView Network Node Manager: Razrabotka i realizaciya korporativnogo resheniya* [OpenView Network Node Manager: Development and implementation of a corporate solution]. Moscow, Internet University of Information Technologies Publ., 2005. 264 p. (in Russian).

28. Zitello T., Williams D., Weber P. *HP OpenView – nastol'naya kniga sistemnogo administratora.* [OpenView – table book system administrator]. Moscow, ECOM Publ., 2006. 616 p. (in Russian).

29. Makarenko S. I. *Spravochnik nauchnyh terminov i oboznachenij* [Handbook of scientific terms and designations]. St. Petersburg, Naukoemkie tekhnologii Publ., 2019. 254 p. (in Russian).

30. Tatomir A., McDermott C., Bensabat J., Class H., Edlmann K. Conceptual model development using a generic Features, Events, and Processes (FEP) database for assessing the potential impact of hydraulic fracturing on groundwater aquifers. Advances in Geosciences. Copernicus GmbH, 2018, vol. 45, pp. 185-192. Doi: 10.5194/adgeo-45-185-2018.

31. Levin V. I. *Strukturno-logicheskie metody issledovaniya slozhnyh sistem* [Structural and logical methods for the study of complex systems]. Moscow, Nauka Publ., 1987. 303 p. (in Russian).

32. Avduevsky V. S. *Nadezhnost' i effektivnost' v tekhnike. Spravochnik v 10-ti tomah. T. 2* "*Matematicheskie metody v teorii nadezhnosti i effektivnosti*" [Reliability and efficiency in engineering. Handbook in 10 volumes. Vol. 2 "Mathematical methods in the theory of reliability and efficiency"]. Moscow, Mashinosroenie Publ., 1988. 280 p. (in Russian).

33. Avduevsky V. S. *Nadezhnost' i effektivnost' v tekhnike. Spravochnik v 10-ti tomah. T. 3* "*Effektivnost' tekhnicheskih sistem*" [Reliability and efficiency in engineering. Handbook in 10 volumes. Vol. 3 "Efficiency of technical systems"]. Moscow, Mashinosroenie, 1988. 328 p. (in Russian).

34. Rudykh S. V. *Sistemy monitoringa i upravleniya sudami tekhnicheskogo i vspomogatel'nogo flota na vnutrennih vodnyh putyah Rossii* [Systems of monitoring and management of vessels of the technical and auxiliary fleet on the inland waterways of Russia]. Dis. for the degree of Doctor of Technical Sciences: 05.13.06. St. Petersburg, Admiral S. O. Makarov State University of the Sea and River Fleet, 2013. 308 p. (in Russian).

35. Budko N. P., Budko P. A., Vinogradenko A. M., Doroshenko G. P., Rozhnov A. V., Mineev V. V., Mukhin A. V. *Sposob raspredelennogo kontrolya i adaptivnogo upravleniya mnogourovnevoj sistemoj i ustrojstvo dlya ego osushchestvleniya* [Method of distributed control and adaptive control of a multi-level system and a device for its implementation]. Patent for the invention RU 2450447 C1, publ. 10.05.2012, bul. No. 13. (in Russian).

36. Pontryagin L. S., Boltyansky V. G., Gamkrelidze R. V., Mishchenko E. F. *Matematicheskaya teoriya optimal'nyh processov* [Mathematical theory of optimal processes]. Moscow, Nauka. Fizmatlit Publ., 1983. 392 p. (in Russian).

37. 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).

Статья поступила 29 сентября 2021 года

Информация об авторе

Будко Никита Павлович – соискатель ученой степени кандидата технических наук. Независимый специалист. Область научных интересов: мониторинг информационных ресурсов; сбор и обработка информации. E-mail: budko62@mail.ru

Адрес: 194064, г. Санкт-Петербург, ул. Бутлерова, д. 9, корп. 3, кв. 252.

Conceptual model of the subsystem of intelligent monitoring of the state of a public information and telecommunications network

N. P. Budko

Problem statement: *based on a multi-level approach to the description of complex technical systems, to substantiate the conceptual modeling of a new generation of network monitoring subsystems.* ***The purpose of the work:*** *to form the principles of construction and functioning of the subsystem of intelligent monitoring of the information and telecommunication network, the general structure and generalized architecture of a promising network monitoring system, as well as to develop its conceptual model in terms of multilevel synthesis of control and diagnostic subsystems.* ***Methods used:*** *methods of multilevel synthesis of complex technical systems; models and methods of reliability theory; methods of object-subject description of information and telecommunication systems; implementation of a functional management model in relation to monitoring subsystems: failure management, configuration management, resource management, performance management, security management; metasystem modeling methods; methods of knowledge representation in complex hierarchical systems.* ***The novelty*** *of the research lies in the fact that in the course of conceptual modeling, the general principles of the functioning of the first monitoring subsystem were formulated; its structure was formed, including sensory, telecommunication and dispatcher levels of its construction in the system aspect; a generalized architecture with an intelligent processing component was proposed, including modules of online analysis, offline analysis and a module of support and decision-making.* ***The result*** *of the conducted research is that the set of requirements and general principles of functioning of a promising monitoring subsystem presented in the work, its structure, in terms of technical and technological foundations of construction, as well as architecture, a gen-*

eral model of a network monitoring subsystem and its generalized model of knowledge representation can be considered as a conceptual model of a new generation intellectual monitoring subsystem on network infrastructures.

Keywords: *information and telecommunications network, monitoring subsystem, logical level of the network, metamodel of a multi-level system, knowledge model, monitoring zone.*

Information about Author

Nikita Pavlovich Budko – Doctoral Student. An independent specialist. Field of research: information monitoring; data acquisition. E–mail: budko62@mail.ru

Address: 194064, Russia, St. Petersburg, Butlerova str., build. 9/3, sq. 252.