УДК 621.39

Общий подход к построению перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей

Аллакин В. В., Будко Н. П., Васильев Н. В.

Постановка задачи: *на основе обзора действующих технологий и существующих систем мониторинга информационно-телекоммуникационных сетей общего пользования, а также анализа научно-методического аппарата оценки временных рядов наблюдаемых метрик, выработать общие требования и подходы к построению перспективных систем сетевого мониторинга и разработать методику прогнозирования (превентивной идентификации) аномальных ситуаций по результатам мониторинга функционального состояния сетевых элементов.* ***Цель работы:*** *выработка общего подхода к формированию методов прогнозирования состояния соединений на информационно-телекоммуникационной сети общего пользования, а также ее сетевых устройств.* ***Используемые методы:*** *методы многомерного анализа данных; методы кластерного анализа; топологические методы анализа временных рядов; методы поведенческой аналитики; символьное представление временных рядов; технологии сетевого мониторинга Site/System Reliability Engineering, как набор инженерных практик, поддерживающих надежную и безотказную работу приложений в настоящем и будущем; Operation Support Systems, как технология поддержки операций; методы системного анализа, структурного синтеза, теории прогноза, теории диагностики, теории классификации.* ***Новизна работы****: для повышения устойчивости и надежности подконтрольной гетерогенной информационно-телекоммуникационной сети ключевым архитектурным принципом проектирования ее подсистемы мониторинга выбран принцип распределенности и децентрализации. Превентивную идентификацию аномальных состояний сетевых элементов, (в виде устройств, каналов, путей и маршрутов) предложено осуществлять путем выявления «запрещенных» кодовых комбинаций при наблюдении временных рядов, которые обрабатываются заимствованными из биоинформатики методами символической динамики, используемыми ранее в процессе анализа сложных нуклеотидных геномных последовательностей, а также введением особого режима мониторинга, когда при идентификации предотказного технического состояния скважность опроса сервером мониторинга сетевого элемента значительно увеличивается с целью своевременного принятия превентивных управляющих воздействий на сетевую инфраструктуру и недопущения пропуска отказа сетевого элемента или наступления аварии на сети. Предложен способ классификации состояния сетевых элементов, состоящий из этапа обучения классификатора на основе EM-алгоритма, а также этапа непосредственно классификации вида технического состояния.* ***Результат:*** *в работе предложена обобщенная архитектура построения перспективных систем сетевого мониторинга, а также общая субъектно-объектная ее модель в виде «сущность-связь». Определены функции подсистемы сетевого мониторинга и сервера мониторинга, как ключевого ее элемента. Рассмотрен вариант структуры сервера мониторинга. Определены назначаемые объекты мониторинга, а также перечень собираемых с них метрических данных с точки зрения функциональной производительности сети. Выбран метод символического представления временных рядов, на основе которого дана оценка энтропии кодовых слов, описывающих временной ряд наблюдаемой метрики функционирующего сетевого элемента, а также разработан алгоритм методики идентификации его аномального состояния на временном ряду параметров, состоящий из четырех этапов: предварительного этапа, этапа кодирования временных рядов, этапа идентификации вида технического состояния сетевого элемента и завершающего этапа.* ***Практическая значимость****: Выработан общий подход к построению алгоритма функционирования перспективных систем сетевого мониторинга.*

Ключевые слова: *временной ряд, децентрализация мониторинга, информационно-телекоммуникационная сеть, подсистема сетевого мониторинга, сервер мониторинга.*

Библиографическая ссылка на статью:
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

Reference for citation:
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 (in Russian). DOI: 10.24412/2410-9916-2021-4-125-227

Актуальность

Развитие информационных технологий (ИТ) в последние десятилетия привело к существенным изменениям в общих подходах к построению и совершенствованию информационно-телекоммуникационных сетей (ИТКС). Ключевыми тенденциями при этом остаются процессы интеграции сетей связи с компьютерными сетями и появление распределенных гетерогенных ИТКС различного масштаба [1], характеризуемых широким внедрением и применением ИТ на базе концепции «Индустрия 4.0» (интернет вещей, «умный город», «умный дом», «умное производство» и пр.), обеспечивающих пользователям предоставление различных инфокоммуникационных услуг на основе стека протоколов TCP/IP, с использованием сетей нового поколения NGN (Next Generation Networks), ядро которых составляют пакетные сети [2]. При этом техническая платформа ИТКС представляется структурированной совокупностью скоростных каналов связи, узлов коммутации, серверов услуг и сервисов связи, действующих в интересах пользователей ИТКС, а также иерархической автоматизированной системы управления связью (АСУС). Фундаментальным же требованием для любой АСУС гетерогенной ИТКС является эффективный *мониторинг* ее ресурсов [3], при котором необходимы точные и актуальные обновления в интересах поддержки своевременной реконфигурации сети (управления сетевыми ресурсами [4]) с целью устранения предотказного ее состояния и недопущения аварии.

Поддержание на высоком уровне эффективности функционирования ИТКС общего пользования на протяжении своих этапов жизненного цикла (ЖЦ) напрямую зависят от значений показателей текущей функциональной надежности ее сетевых элементов и сегментов [5]. Последствия возникновения отказов или дефектов в ИТКС, обслуживающих отрасли с критически важными инфраструктурами (КВИ), могут привести к глобальным катастрофам и трагедиям с большими человеческими жертвами или значительным экологическим и финансовым ущербом.

В связи с чем, на сегодня в телекоммуникационной отрасли активно ведется разработка новых технологий поддержания функциональной безопасности ИТКС и систем, направленных на обеспечение их эксплуатационной надежности, а вопросам проведения мероприятий по диагностике и мониторингу технического состояния (контролю) уделяется первостепенное значение. Так, например, на внедрение методов неразрушающего контроля на эксплуатационных этапах ЖЦ атомной электростанции затраты могут составлять до 50 % всех эксплуатационных затрат [6].

Категоричность современных экологических нормативов и требований общественности о необходимости исключения техногенных аварий и катастроф с человеческими жертвами и огромным ущербом для окружающей среды делает проблему поддержания надежности и функциональной безопасности ИТКС актуальной, а разработку систем мониторинга функционального состояния их элементов – приоритетной.

Согласно [7] под *мониторингом технического состояния* (ТС) понимается составная часть технического обслуживания, заключающаяся в наблюдении за объектом с целью получения информации о его ТС и рабочих параметрах.

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

Одной из мало исследованных и еще нерешенных задач является построение подсистемы мониторинга процессов функционирования территориально-распределенных систем различной сложности. При этом, современные ИТКС как общего пользования (ОП), так и специального назначения (СН) [8] можно всецело отнести к гетерогенным сетям, что также накладывает определенные трудности и особенности построения их подсистем мониторинга (под *гетерогенными* называют, как правило сетевые структуры, образующиеся посредством объединения различных ведомственных сетей, имеющих разные принципы построения, сетевые технологии доставки и/или защиты информации, и /или программно-аппаратные средства [1]). Действительно, гетерогенность (неоднородность) сети предполагает несовместимость узлов, принадлежащих одной сети, либо к смежным сегментам сети по одному или нескольким логическим признакам: по типу применяемых операционных систем, форматам кадров сети, моделям безопасности, способам защиты информации и пр. Из чего следует, что в гетерогенных ИТКС подсистема мониторинга должна строиться на основе принципов *децентрализации* и *многоуровневости*. Притом, что ИТКС, как правило, имеет строго иерархическую структуру, ее подсистема мониторинга должна позволять осуществлению перераспределения функций центра управления функционированием и периферией в зависимости от текущего состояния всей системы.

В последние годы объективные процессы государственного управления и динамика принятия решений являются таковыми, что ведомственная обособленность ИТКС становится тормозом развития страны и потому нуждается в коренном изменении. Одной из специфики таких гетерогенных сетевых инфраструктур отмечается то, что они носят, как правило, межведомственный характер. Причем создание межведомственных ИТКС сопряжено с рядом особенностей [9-11], отличающих их от традиционных сетей связи, среди которых:

– географическая рассредоточенность ресурсов сети, а также источников и получателей информации;
– пульсирующий характер сетевого трафика;
– разнородность элементов и применяемых сетевых технологий;
– невозможность полного математического описания (построения полноценной математической модели) как мультисервисной ИТКС в целом, так и отдельных телекоммуникационных сетей в ее составе, при несомненной необходимости в этом;
– случайность функционирования ИТКС, влекущая за собой трудности при проведении анализа ее состояния (мониторинга) и организации управления;

– существенная нестационарность, что вызывает разную реакцию сети на одну и туже ситуацию или управление в различные моменты времени;
– необъяснимая «нетерпимости» к управлению, под которой понимается то, что гетерогенная сеть связи предназначена для сопряжения и передачи информации, а не для управления ею, т. е. функционирует независимо от системы управления.

Сложность и актуальность создания подсистем мониторинга для таких гетерогенных ИТКС сопряжена наряду с их особенностями еще и рядом ограничений, среди которых можно выделить следующие: наличие разнородных протоколов взаимодействия между узлами и периферийными сетевыми устройствами, постоянные трансформации сетевых топологий и структур сети, сопряжение сегментов маломощных и высокопроизводительных элементов сети, широкое применение носимых (мобильных) станций и устройств со слабой вычислительной мощностью, низким энергопотреблением, малым объемом памяти.

Все эти особенности позволяют вести речь о несовершенстве существующих систем контроля, ориентированных на применение в гомогенных сетевых структурах и необходимости поиска новых технологий и подходов к построению систем распределенного мониторинга функционального состояния современных гетерогенных сетей связи, включая методы интеллектуального мониторинга.

Цель статьи: на основе общего обзора действующих систем сетевого мониторинга, а также методов анализа временных рядов, разработать методический аппарат (комплекс методов) превентивной идентификации аномального состояния информационно-телекоммуникационной сети общего пользования, и выработать общие принципы, а также требования к построению систем мониторинга нового поколения.

Введение

В современных системах мониторинга динамика объекта управления (сетевого элемента, канала, сети) представляется как последовательность переходов между стационарными состояниями. Примеры данного утверждения помимо уже указанного ГОСТ 27.002-2015 [7], даются также и в рекомендации М.3703 Международного Союза электросвязи (МСЭ) [12], где вводятся следующие виды состояний:

– «неопределенное» (Undefined, *U*);
– «норма» (Normal, *N*);
– «незначительное нарушение» (Minor, *I*);
– «значительное нарушение» (Major, *J*);
– «критическое» (Critical, *C*);
– «авария» (Fault, *F*).

Основная задача системы мониторинга состоит в оперативном событийном уведомлении лица, принимающего решение (ЛПР), или оператора подсистемы мониторинга ИТКС, об изменении ее состояния. Как правило, в конечной интерпретации ЛПР таких состояний всего два «норма» – сетевой элемент выполняет свои функции и «авария» – сетевой элемент не может выполнять свои

№4. 2021
ISSN 2410-9916

функции. Остальные состояния служат для уведомления ЛПР о направлении динамики процесса – от «нормы» к «аварии» и от «аварии» к «норме».

Переходный процесс от «нормы» (*N*) к «аварии» (*F*) редко характеризуется явной последовательностью событий *N* – *I* – *J* – *C* – *F*. Как правило, в журнале событий будет наблюдаться переходный процесс с колебаниями. Возможен как временный возврат на менее критическое состояние, так и резкие скачки «через» состояние, которое не было идентифицировано по причине малой скважности опроса системой мониторинга. Наиболее используемым в системах мониторинга является триггерный механизм (или метод гестерезиса) [13] идентификации состояния, который позволяет устранить дублирование событий в журнале в случае колебаний измеримой характеристики вблизи порога (т. н. эффект «дребезга нуля»). Метод заключается в назначении пары пороговых значений «возрастающего» и «убывающего» порогов. Событие генерируется, когда превышается «возрастающий» порог. Как только этот порог превышен, событие не генерируется снова, пока не будет пересечен «убывающий» порог. Наглядно метод гистерезиса показан на рис. 1.

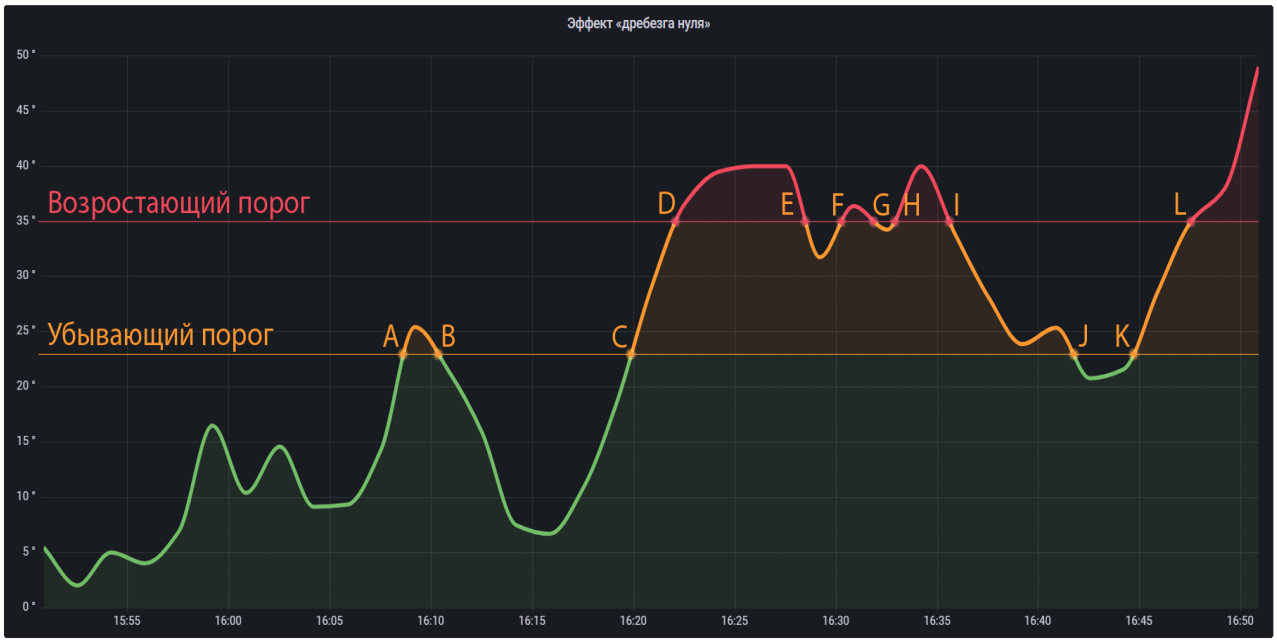


Рис. 1. Демонстрация применения триггерного механизма для уменьшения числа событий вследствие эффекта «дребезга нуля»

Поскольку начальное состояние было настроено на срабатывание при повышении «возрастающего» порога, в точке *A* сигнал тревоги не генерируется. По мере того, как значение измерения увеличивается до уровня выше «возрастающего» порога, сигнал тревоги генерируется в точке *D*. Никаких сигналов в точках *E*, *F*, *G*, *H* или *I* не генерируется до тех пор, пока не будет сгенерирован сигнал о пересечении «убывающего» порога (точка *J*). И снова в точке *K* не будет генерироваться никаких дополнительных сигналов тревоги, пока не произойдет пересечение «возрастающего» порога в точке *L*. В итоге, без гистерезиса было бы сгенерировано 12 аварийных сигналов, с гистерезисом генерируются только три. Зачатую, сокращение генерации аварийных сигналов бывает бо-

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

лее значительным. Однако данный механизм гистерезиса не приводит к надежной идентификации направления динамики процесса.

Предметом данного исследования являются алгоритмы и методы выявления нестационарных состояний объекта мониторинга, на котором проводится измерение. В этой постановке сформулированы и решаются следующие задачи:

- анализ рынка межведомственных систем сетевого мониторинга;
- обзор методов анализа временных рядов;
- символьное кодирования значений временного ряда и способ кодирования участков (ячеек) временного ряда вектором оценок энтропии сдвигов;
- метод обучения классификатора состояний объекта измерения на основе энтропии сдвигов;
- метод классификации состояния по тестовой выборке измерений при описании измеряемой характеристики сетевого элемента распределением вероятностей сдвигов;
- метод реконструкция состояния каналов связи средствами сетевой томографии;
- метод классификации состояния информационно-телекоммуникационной сети;
- алгоритм методики превентивной идентификации состояния сетевых устройств на основе символьного представления временных рядов их метрик;
- модельный пример работы алгоритма (вычислительный эксперимент);
- алгоритм методики синтеза подсистемы интеллектуального мониторинга информационно-телекоммуникационной сети ситуационного центра ведомства.

1. Основные обозначения и терминологический аппарат

При проведении обзора научных методов построения перспективной системы мониторинга ИТКС ОП, а также в ходе решения вышеперечисленных частных задач в работе вводятся следующие условных обозначения, показанные в таблице 1. Терминологический аппарат, раскрывающий типы сущностей, процессов, объектов и субъектов системы мониторинга, используемый в ходе исследования представлен в таблице 2.

Таблица 1 – Основные обозначения

Обозначение	Физический смысл обозначения
$X = (x_i, t_i)$	– временной ряд характеристики (параметра) сетевого элемента, полученной путем измерений
x_i	– значение характеристики (параметра) сетевого элемента в момент t_i, $x_i \in R$, $i = \overline{1,n}$; n – число наблюдений (временных отсчетов)
$f(x\|\theta)$	– функция плотности вероятности распределения значений односторонних задержек на сети
θ_k	– набор параметров θ_k компонентов (K сетевых элементов) сети, $k = \overline{1,K}$

Обозначение	Физический смысл обозначения
μ_k, σ^2_k	– соответственно среднее значение и дисперсия выборки значений параметров на векторе X
π_k	– априорная вероятность, что измеренное состояние принадлежит k-му компоненту, $C = k$
$p(h)$	– плотность распределения вероятностей энтропии сдвигов
$L(\theta)$; $L(\theta)>\varepsilon$	– логарифмическая функция правдоподобия и критерий ее сходимости, $\theta \in \{\pi_k, \mu_k, \sigma^2_k\}$
z_{ik}	– априорная вероятность после наблюдения x_i, созданного компонентом k
$P(H\|C = k)$	– вероятность принадлежности выборки $H = (h_1, ..., h_n)$ состояниям C_k
$P(C=k\|H)$	– вероятность того, что полученная проекция энтропии H произведена k-й компонентой
$\sum_{знач}$; $\sum_{тенд}$	– алфавит кодирования временного ряда по его значениям и тенденциям
C_m; $C(m)$	– оценка энтропии слов и оценка энтропии сдвигов, соответственно
$g = (V, E, \alpha, \beta)$	– граф, описывающий сеть и представляемый: множеством вершин (узлов) V, множеством дуг E, функцией разметки узлов α: $V \rightarrow L_V$, функцией разметки ребер β: $E \rightarrow L_E$
$d(g, g')$	– расстояние между графами
$G=\{g_1,g_2,\ldots,g_n\}$	– медианный граф с минимальным суммарным расстоянием от центра масс до других графов
$c(e)$	– стоимость операции e редактирования графа (под операцией понимаем замену метки узла, замену метки дуги, вставку узла, вставку дуги, удаление узла, удаление дуги)
$[t, t+1]$	– временной интервал наблюдения за графом (за временным рядом метрики)
$g_1^{\max} = \{\alpha, \beta\}$	– максимально общий подграф графа g и g_2 (maximal common subgraph – MCS)
$\rho(g)=(L,C,\lambda)$	– представление графа в метках, где $L = \{\alpha(x)\| x \in V\}$, $C = \{\alpha(x), \alpha(y)\| (x, y) \in E\}$, $\lambda(\alpha(x), \alpha(y)) = \beta(x, y)$ для всех дуг $(x, y) \in E$
$\boldsymbol{A_g}$ $\{\lambda_1,\lambda_2,\ldots,\lambda_n\}$	– матрица смежности вершин графа g
$\sigma(g)$	– спектр графа (последовательность собственных чисел матрицы $\boldsymbol{A_g}$ смежности вершин
$P^g = \mathrm{U}_{k \geq 2} P_k^g$	– совокупность всех путей k длины большей 2 соединяющих вершины графа g
$C = [C_{uv}]$	– матрица изменений, элементы которой соответствуют удаленным из графа g_1 или добавленным в граф g_2 элементам (узлам, дугам)
$g_1 \Delta g_2$	– симметричная разница графов
$\varphi_1, \varphi_2, \ldots, \varphi_m$	– набор пороговых значений
d: $X \in R^d$	– принадлежность множества точек X евклидову пространству размерности d
$N–I–J–C–F$	– виды состояний сетевых устройств в соответствии с рек. M3703 [12]: «неопределенное» (Undefined, *U*); «норма» (Normal, *N*); «незначительное нарушение» (Minor, *I*); «значительное нарушение» (Major, *J*); «критическое» (Critical, *C*); «авария» (Fault, *F*)
$F–C–A–P–S$	– модель функциональной безопасности сети: (*F*) Fault Management / Управление отказами; (*C*) Configuration Management / Управление конфигурацией; (*A*) Accounting Management / Учёт; (*P*) Performance Management / Управление производительностью; (*S*) Security Management / Управление безопасностью
GED	– расстояние редактирования графа (graph edit distance)
msa; *mma*; *msd*; *mmd*	– процедуры сравнения среднего графа, соответственно, с последующим одиночным; с последующим средним; с удаленным одиночным; с удаленным средним

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

Сущность, процессы, объекты, субъекты	Характеристика, описание, физический смысл сущности, процесса, объекта, субъекта системы мониторинга
Основные типы сущностей	
«Интерфейс»	Набор средств, используемых для взаимодействия двух систем. Англ. «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 при сравнении измерения с пороговым значением. События характеризуют: классом; временем генерации; адресом, при обращении к которому сгенерировано событие; идентификатором программного компонента, сгенерировавшего 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 управления 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» в составе:	В системе 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»

2. Концептуальная модель объектов управления в системах мониторинга. Объектно-субъектное описание

Проведенный детальный анализ реализации на уровне систем управления базами данных (СУБД) систем мониторинга методов моделирования ИТКС ОП показывает наличие двух основных подсхем: схемы *объектов управления*, описывающих контролируемые каналы, интерфейсы, сети и схемы *субъекта управления* (конфигурация измерительного агента) [14].

Модель объекта управления. Базовыми объектами CIM (Common Information Model – общая информационная модель), GMPLS (Generalized MultiProtocol Label Switching – протокол и модели, разработанные комитетом 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:

– 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 управле-

№4. 2021
ISSN 2410-9916

ния. Тогда обобщенная объектная модель в виде «сущность-связь» будет имеет вид, представленный на рис. 2.

Рис. 2. Обобщенная объектная модель в виде «Сущность-связь»

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.

3. Анализ рынка межведомственных систем сетевого мониторинга

Рассмотрим некоторые из существующих систем сетевого мониторинга.

System Center Operations Manager (SCOM) [15] – система сквозного мониторинга (от Microsoft) и активного наблюдения за любыми сетевыми устройствами, поддерживающими протокол обмена информацией SNMP (до уровня порта), обнаружения виртуальных локальных вычислительных сетей (VLAN) и коммутаторов в них, слежения за их техническим состоянием.

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

В последних версиях Microsoft SCOM появилась возможность наблюдения не только за устройствами под управлением операционных систем (ОС) семейства Windows, но и за гетерогенными средами, включая UNIX и Linux. SCOM предназначен в основном для организаций с числом сетевых устройств более 500 и числом серверов более 30. Для организаций меньшей структуры существует продукт System Center Essentials, включающий в себя часть функций SCOM и System Center Configuration Manager, но предназначенный для ИТКС малых и средних предприятий. В последнее десятилетие SCOM относят к сервису высокой доступности, благодаря отсутствию серверов управления. При сопряжении с несколькими серверами нагрузка балансируется, обеспечивая доступность. При этом на каждом из серверов работает служба конфигурации, а хранение данных реализовано не в памяти или XML-файлах, а в базе данных (БД). Microsoft также предоставляет возможность интеграции SCOM с System Center Service Manager, благодаря чему у пользователя есть возможность автоматического создания инцидентов на основе оповещений SCOM. Для слежения за виртуальными средами SCOM интегрируется с пакетом System Center Virtual Machine Manager, откуда получает информацию о частных облаках, виртуальных машинах и службах.

К основным преимуществам SCOM можно отнести:

– высокую производительность и работоспособность в среде Microsoft;
– обеспечение сквозного управления службами для сервисов ЦОДа;
– унифицированный контроль частных и общедоступных облачных сервисов;
– существенное повышение эффекта в управлении средой ЦОДа;
– поддержку Windows PowerShell 2.0 с набором новых командлетов [15].

Но одним из главных достоинств SCOM является продвинутая визуализация всего собранного набора метрик и представление их в виде графиков и диаграмм, что доступно как в специальной консоли программы, так и через web-интерфейс.

Однако SCOM имеет и ряд недостатков с точки зрения решения своего функционала [15]:

– она охватывает множество общих показателей системы, но непригодна для слежения за специфическими параметрами;
– до сих пор работа с ОС вне семейства Windows нестабильна;
– требует установки сервиса агента;
– существенная громоздкость и трудоёмкость настройки «под себя» – система больше подходит для мониторинга общего состояния и сбора основных сведений о глобальной структуре (числе клиентских и серверных машин в домене и пр.).

Сюда же можно отнести высокую стоимость данного программного обеспечения (ПО).

Zabbix [16] – свободно распространяемая система для проведения комплексного мониторинга сетевого оборудования, серверов и сервисов, состоящая из элементов:

– *сервер мониторинга* (ядро), выполняющий периодический опрос и сбор данных, их обработку и анализ, а также осуществляющий запуск скриптов для отправки оповещений. С его помощью можно удаленно контролировать сетевые сервисы. Он является хранилищем, в котором собраны конфигурационные, статистические и оперативные данные. Однако он не предназначен к размещению на сервере под управлением ОС семейства Windows и OpenBSD;
– *прокси* – осуществляет сбор данных о доступности и производительности от имени Zabbix-сервера. Полученные данные заносятся в буфер на локальном уровне и передаются Zabbix-серверу, которому принадлежит прокси-сервер. Zabbix-прокси является эффективным решением для централизованного удаленного мониторинга филиалов и сетей, не имеющих локальных администраторов. Он может быть также применен для распределения нагрузки одного Zabbix-сервера. Причем прокси лишь собирает данные, т. е. на сервер ложится меньшая нагрузка (на его устройства ввода/вывода диска и на центральный процессор устройства – ЦПУ);
– *агент* – специальное программный процесс, запускаемый на объектах мониторинга и представляющий данные серверу по приложениям и локальным ресурсам на сетевых системах (статистика процессора, жесткие диски, память, и т. д.), которые должны работать с запущенным Zabbix-агентом. Однако мониторинг можно осуществляться не только с помощью него, но и по SNMP (версии 1-3), запуском внешних скриптов, выдающих данные, и некоторые виды предопределенных встроенных проверок, таких как ping, запрос по протоколам http, ssh, ftp и пр., а так же измерение времени ответа этих сервисов. Zabbix-агенты являются достаточно эффективными из-за применения встроенных системных вызовов для сбора информации о статистике и поддерживаются как на *nix ОС, так и на AIX, Windows;
– *Web-интерфейс* – средство визуального представления Zabbix, рис. 3.

С помощью Zabbix обычно осуществляют распределённый мониторинг до 1000 узлов, где конфигурация младших узлов в иерархии контролируется старшими. Также продукт включает централизованный мониторинг логфайлов. При этом имеется возможность создавать вручную по шаблону карты сетей, выполнять запросы в различные БД, генерировать отчёты и выявлять тенденции изменения метрик, выполнять сценарии на основе результатов мониторинга, поддерживать интеллектуальный интерфейс управления платформами (IPMI).

В качестве преимуществ Zabbix можно выделить то, что она позволяет осуществлять:

– автоматическое обнаружение IP-адресов по диапазону;
– доступные сервисы;
– проведение SNMP проверок;

– автоматическое удаление отсутствующих хостов и автоматический мониторинг обнаруженных сетевых устройств с распределением их по шаблонам и группам и др.

Рис. 3. Вариант карты сетей в Zabbix

В качестве недостатков Zabbix стоит отметить:

– громоздкость сервиса;
– отсутствие полной документированности возможностей;
– необходимость установки Zabbix-агентов на все машины, сложность делегирования прав.

Так, машина с сервисом зачастую управляется ОС семейства *nix, что делает трудоёмким взаимодействие с доменными пользователями и правами из Active Directory (Windows).

Nagios [17] – свободно распространяемое ПО для мониторинга ИТКС и изначально разработанное для ОС на базе Linux, однако эффективно работает под Sun Solaris, HPUX, FreeBSD, AIX. С помощью Nagios доступны: комплексный мониторинг за ИТ-инфраструктурой, мониторинг безопасности ИТКС, возможность оповещать администратора сети о получаемых данных в ходе наблюдения, выявление проблем сразу после их возникновения, что сокращает время простоя и коммерческие потери.

Также к достоинствам Nagios относят:

– мониторинг сетевых служб (SMTP, HTTP, SNMP, POP3, NNTP, ICMP);
– мониторинг состояния хостов в большинстве сетевых ОС (загрузка процессора, системные логи, использование диска);
– поддержка удаленного мониторинга через шифрованные туннели SSH, SSL;
– возможность построения карт сетей, рис. 4;

– простая архитектура плагинов (модулей расширений) позволяет разрабатывать свои собственные способы проверки служб, используя любой язык программирования по выбору;
– параллельный мониторинг служб;
– возможность определения иерархии хостов сети с помощью «родительских» хостов, что позволяет обнаруживать и различать хосты, вышедшие из строя, или которые недоступны;
– отправка оповещений при возникновении проблем со службой или хостом через модуль системы с помощью почты, sms, или иным способом, определяемым пользователем;
– осуществление автоматической ротации лог-файлов;
– определение обработчика событий, возникающих с хостом, для разрешения проблем;
– возможность создания распределенной системы мониторинга путем организации совместной работы нескольких систем мониторинга с целью повышения эффективности.

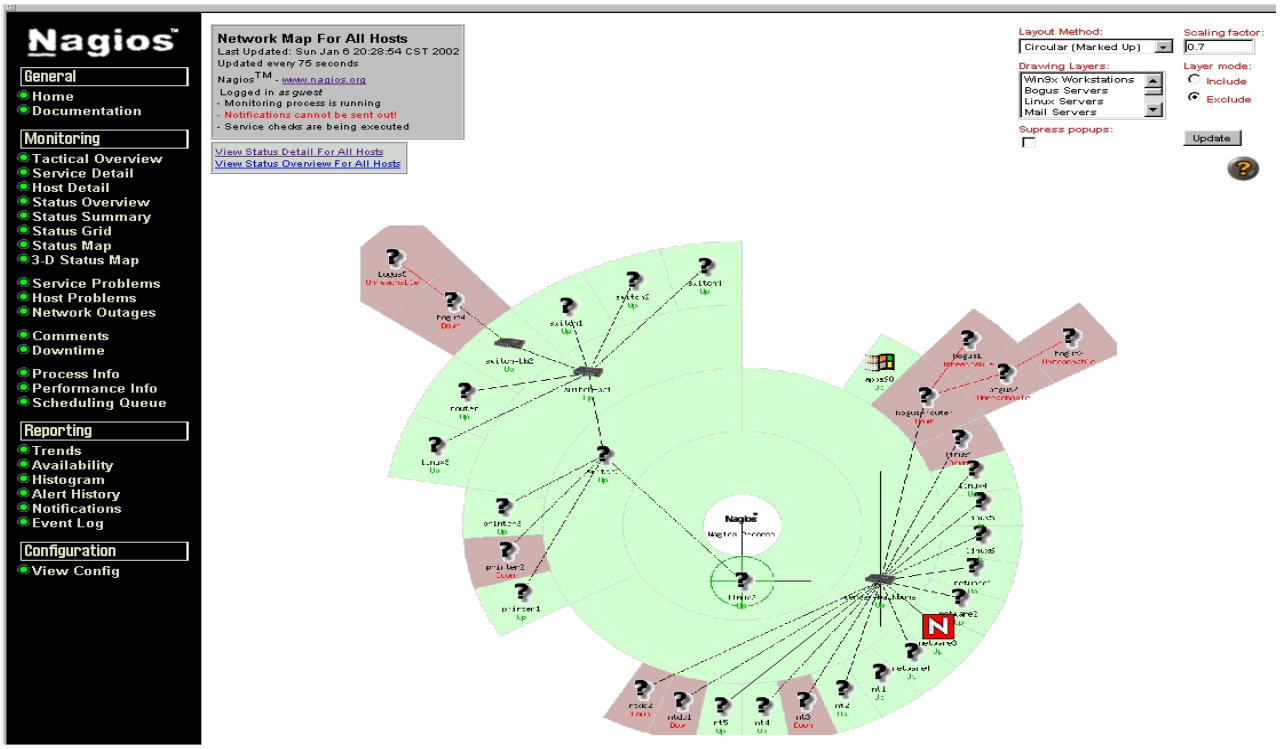


Рис. 4. Вариант карты сетей в Nagios [17]

К недостаткам использования Nagios можно отнести:
– достаточно скудную функциональность «из коробки», влекущую за собой «общий» характер мониторинга и его «сетевую» направленность;
– необходимость поиска и установки расширений для создания полнофункциональной системы мониторинга (например, автоматическое раскрытие топологии сети, сбор, визуализация и обработка данных временных рядов (rrdtool));

– отсутствие функционала интеграции со средствами мониторинга каналов (точка-точка) как на уровне модели данных, так и на уровне отображения;
– ориентация с точки зрения визуализации на устройства и сервисы, средств абстрагирования при переходе от детального отображения сети к высокоуровневому;
– проблемы взаимодействия с серверами под ОС Windows.

Cacti [18] – бесплатное приложение мониторинга, которое позволяет собирать статистику по метрикам за определённые временные интервалы с отображением их в графическом виде при использовании утилиты RRDtool, предназначенной для функционирования с круговыми базами данных (типа Round Robin Database) и использующейся для хранения информации об изменении одного или нескольких параметров за определенный промежуток времени. Стандартно шаблон сбора включает статистику по загрузке процессора, количеству запущенных процессов, использованию входящего/исходящего трафика, выделению оперативной памяти.

Cacti написан в инфраструктуре Apache-PHP-MySql с возможностью дописывания собственных агентов сбора данных и настройкой сбора и отображение данных мониторинга. При этом интерфейс отображения статистики метрик, собранной с сетевых устройств, представлен деревом, структура которого может задаваться самим пользователем. Как правило, статистика группируется по заданным критериям, причем один и тот же график может присутствовать в разных ветвях дерева или рассматриваться отдельно, с представлением горизонта времени: последний день, неделя, месяц и год (или иной временной промежуток). Имеется режим предпросмотра (просмотр заранее составленного набора графиков), рис. 5.

Достоинства Cacti:
– высокая скорость развертывания при минимальном кодировании;
– простота и удобство интерфейса настройки просмотра отчетов.

Недостатки Cacti:
– быстрый рост числа типовых настроек при большом количестве сред и серверов;
– ограниченная производительность «неродных» JMX решений;
– невозможность инвентаризации при перераспределении ресурсов сети.

Cacti позволяет для нескольких пользователей разграничить их права, как на просмотр статистики, так и на управление системой. В тоже время Cacti позволяет строить графики только основных показателей производительности, поскольку мониторинг нестандартных метрик значительно снижают производительность ПО.

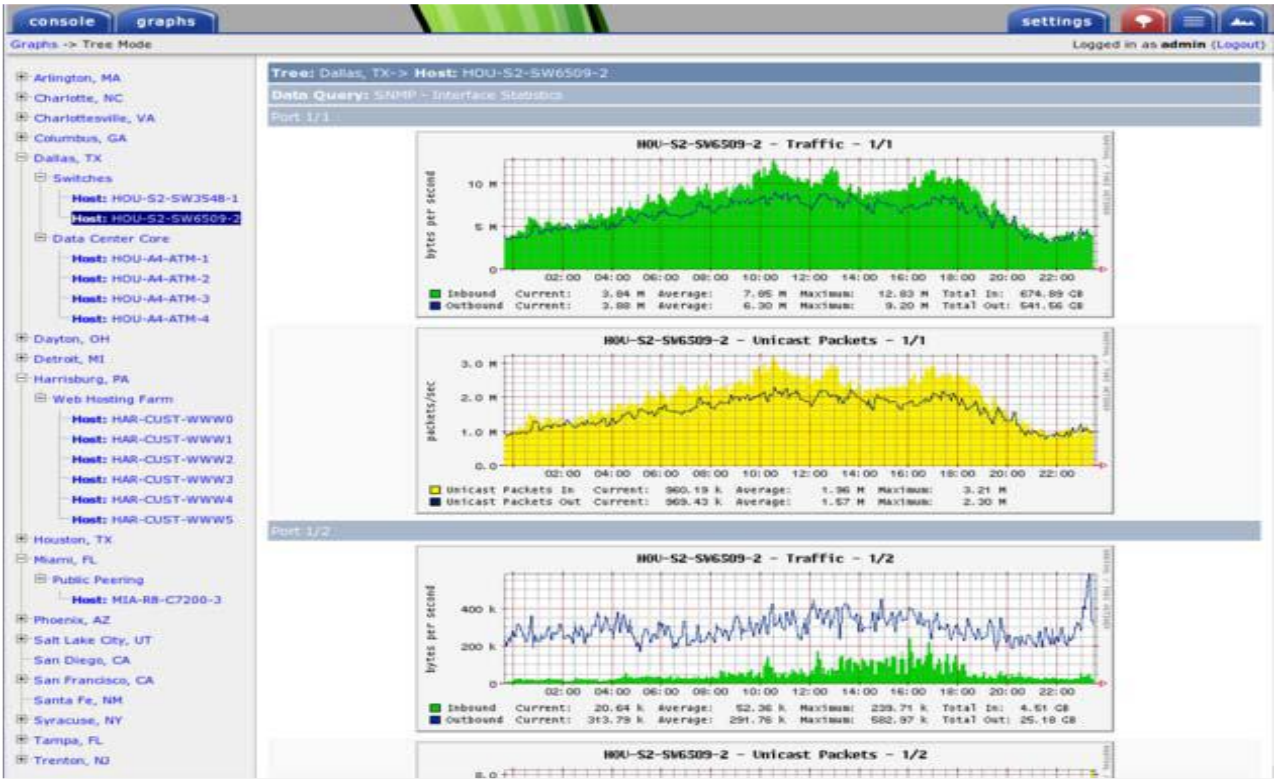


Рис. 5. Интерфейс Cacti [18]

Prometheus – свободно распространяемое ПО в интересах мониторинга сетевых устройств, серверов и сервисов с встроенным базовым интерфейсом, но чаще используется в связке с сервером визуализации данных ***Grafana***, рис. 6.

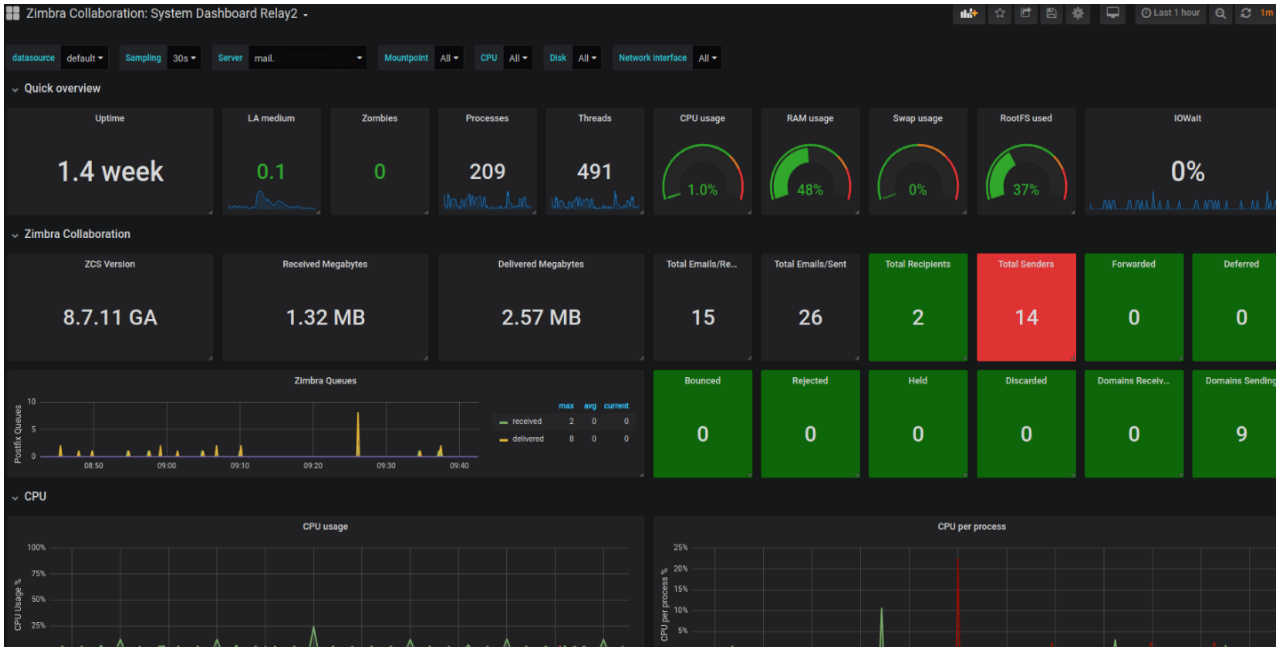


Рис. 6. Web-интерфейс сервера визуализации данных Grafana

В состав Prometheus входят:

– *сервер мониторинга* – выполняет периодический опрос и сбор данных с элементов сети, а также их обработку и анализ. При обнаружении

аномалии осуществляет обращение к интерфейсу оповещения оператора. С помощью сервера мониторинга также удаленно контролируются сетевые сервисы. Фактически сервер мониторинга является хранилищем, в котором собраны конфигурационные, статистические и оперативные данные по структуре сети и функциональному состоянию сетевых элементов. Имеет удобный интерфейс для доступа к данным в случае интеграции с другими сервисами (интерфейс оповещения, интерфейс отображения). Как недостаток отметим, что он не предназначен к размещению на сервере под управлением операционной системы (ОС) семейства Windows;

– *экспортер* (*exporter*) – элемент сервера мониторинга, осуществляющий сбор данных о доступности и производительности объектов мониторинга. Существует множество экспортеров предназначенных для сбора метрик из всех видов ОС и для сбора метрик из конкретных программных продуктов. При необходимости кастомизации может быть дописан самостоятельно для реализации отправки метрик элементу Pushgateway. Предоставляет *web*-интерфейс для доступа к метрикам объекта мониторинга, который опрашивается сервером мониторинга;
– *Pushgateway* – специальное ПО, предназначенное для приема метрик от объекта мониторинга (агента), и представляющее их для сбора сервером мониторинга;
– *Alert manager* – элемент сервера мониторинга, принимающий сигналы об аномалиях, и принимающий решение об использовании той или иной схемы оповещения ответственных лиц.

Operation Support Systems (OSS) [14] – системы поддержки операций, построенные на базе протокола SNMP (версий 1 и 2). Используются ведущими телекоммуникационными компаниями.

В рассматриваемой высокоуровневой архитектуре OSS Hewlett-Packard (HP) OpenView-NNM [19], OpenNMS, а также Huawei U2000LCT, центральным компонентом OSS является компонент диспетчеризации событий, совмещенный с настраиваемым классификатором событий, отказов и предупреждений (рекомендация M.3703 [12]).

Данная OSS-технология более подробно будет рассмотрена ниже.

Еще одной из технологий все более настойчиво завоевывающей рынок IT-услуг для телеком-операторов и направленной на поддержание эксплуатационной надежности ИТКС и систем, является технология ***SRE*** (***Site/System Reliability Engineering***), рассматриваемая в виде набора инженерных практик, поддерживающих надежную и безотказную работу приложений в настоящем и будущем [20]. Данная технология ориентирована на способность обнаруживать аномальные ситуации и проблемы в работе ИТКС до того, как о них сообщат абоненты. Концепция SRE-технологии ориентирована на решение внутренних задач ИТКС с измерением времени безотказной работы ее сетевых элементов и сервисов, а также точного определения их доступности с учетом требований по масштабируемости и внезапным форс-мажорам. Технология SRE предполагает устранение организационных барьеров между функциями специалистов по раз-

работке специального ПО и по информационно-технологическому обслуживанию ИТКС с учетом взаимной интеграции их рабочих процессов друг в друга, как при использовании единых индикаторов оценки функциональной безопасности, так и общей ответственности всех участников предоставления информационно-телекоммуникационных услуг на этапах ЖЦ ИТКС.

К примеру, индикаторами доступности SRE являются такие метрики как:

– SLI (Service Level Indicator) – пропускные способности, задержки запросов, количество запросов в секунду, число сбоев на запрос. Данные метрики сначала агрегируются во времени и переводятся в среднее (или в %) по сравнению с порогом;
– SLO (Service Level Objective) – целевые показатели метрик времени SLI за отчетный период времени: сутки, неделя, месяц, квартал, год и пр.

При этом важно отметить, что всякие простои сети грозят телеком-оператору убытками, в связи с чем, необходимо предоставлять текущие значения метрик SRE в режиме on-line [21]:

– RPO (Recovery Point Objective) – максимальный период времени, за который могут быть потеряны данные в результате инцидента (целевая временная точка восстановления ИТКС). Для телеком-оператора данный показатель необходимо минимизировать, и, в идеале, свести к нулю, RPO → 0. Такие инструменты, например, как автоматическая репликация данных в файловой системе снижает RPO, но для высокой доступности всего сервиса только этого недостаточно. Вычисление значения RPO относится к задачам DevOps- и SRE-инженеров;
– RTO (Recovery Time Objective) – интервал времени, в течение которого ИТКС может быть недоступной в случае отказа или аварии (целевое время восстановления системы). Данное время необходимо для восстановления полного функционирования системы (сервиса) после возникновения аварии. SRE-инженеры должны организовать систему так, чтобы с использованием различных технологий отказоустойчивости и восстановления данных из резервных копий восстановить работоспособность системы на резервном сервере (оборудовании), площадке. Задачей оптимизации является минимизация значений RPO и RTO.

Внедрение систем мониторинга в корпоративных ИТКС особо важно при использовании в деятельности ИТ-подразделений сервисного подхода [22], когда все процессы поддержания функциональной надежности просматриваются с точки зрения предоставляемых подразделением ИТ-сервисов. Каждый бизнес-сервис корпоративной ИТКС по возможности интерпретируют как ИТ-сервис и описывают в системе мониторинга набором взаимосвязанных компонент ИТ-инфраструктур, с определением уровня качества предоставления пользователю.

Таким образом формируют Соглашение об уровне качества сервисов (SLA – Service Level Agreement), согласно которому система осуществляет сбор и хранение информации о качестве предоставления ИТ-сервисов. На базе накопленных метрик формируются отчеты за заданный период времени, анализ которых помогает осуществлять: пересмотр уровня предоставления ИТ-

сервисов, реорганизацию деятельности ИТ-подразделения, модернизацию ИТ-инфраструктуры.

Одной из задач технологии SRE является вычисление и поддержание заданного уровня доступа к сетевым элементам ИТКС с уточнением, какие именно ее показатели надежности должны быть под постоянным мониторингом, измерением и оценкой. Обычно в SLA-договоре между поставщиком телекоммуникационной услуги и ее получателем [20] при описании процесса управления доступом указывают следующие контрольные метрики оценки качества ИТ-сервиса: доступность (availability); производительность (performance); надежность (reliability); сопровождаемость (maintainability); обслуживаемость (serviceability); безопасность (security) [23]. При этом в SLA-договоре устанавливается регламент взаимоотношений с потребителями услуг, в то время как SRE-технология необходима в первую очередь для внутреннего пользования и взаимодействия служб технической поддержки ИТКС. Поэтому требования, предписанные к качеству сервиса SRE-стандартом, как правило, выше указанных в SLA-договоре [24].

Для обеспечения эффективного взаимодействия между двумя ИТКС или двумя ее сегментами, как правило, используют встроенные средства контроля и управления внутри ореола их действия (мониторинг OSS), а в точках демаркации – независимые измерительные средства контроля (мониторинг SLA). Таким образом, область применения систем мониторинга SLA и контроля качества сводится к совокупности точек демаркации. В иных точках нет потребности контролировать показатели сети независимыми средствами, поскольку встроенные системы управления и самодиагностики (фактически уровня NMS) решают эту задачу в полной мере. Это позволяет сформировать идею практического минимума системы управления: вместо развития глобальной системы по пути NMS-TMN-OSS и далее можно остановиться на ее первом шаге NMS – системе управления сетью (Network Management Systems); связь NMS друг с другом можно оформить в виде отдельных соглашений в SLA-договоре; дополнить полученную систему мониторинга системой мониторинга SLA и создать «лоскутное одеяло» в виде NMS, соединенных каналами информационного взаимодействия.

Такая конструкция существенно уступит информационным системам разного уровня управления, рассмотренным выше, но ее преимущество состоит в стоимости решения и времени развертывания. Предложенную систему управления можно развернуть в течение 2-3 недель без привлечения ресурсов внешних специалистов или системных интеграторов. При этом она будет достаточно разнообразной по составу сетевого оборудования и охвату географии его размещения.

Территориальное ограничение применения систем мониторинга SLA в ИТКС не должно рассматриваться как уменьшение их значимости. Эти средства контроля применяют только в точках демаркации на границах подсетей, но в настоящее время количество таких точек растет с увеличением номенклатуры систем, разного оборудования, сервисов, и др. Причем область квалиметрии и метрологии в точках демаркации, наоборот, расширяется по мере развития ИТ.

№4. 2021
ISSN 2410-9916

При этом географическое ограничение сферы применения мониторинга SLA в системе позволит направить решение задач контроля качества, не вторгаясь в область систем управления OSS.

Выделяют три варианта точек демаркации [25] (рис. 6): «оператор-оператор» – точка при взаимодействии операторов, «оператор-пользователь» – точка подключения клиента, а также внутренние точки демаркации (между производителями, между структурными или регламентными подразделениями ИТКС). В этом случае для определения внутренних точек демаркации действует соглашение операционного уровня – OLA (Operational Level Agreement).

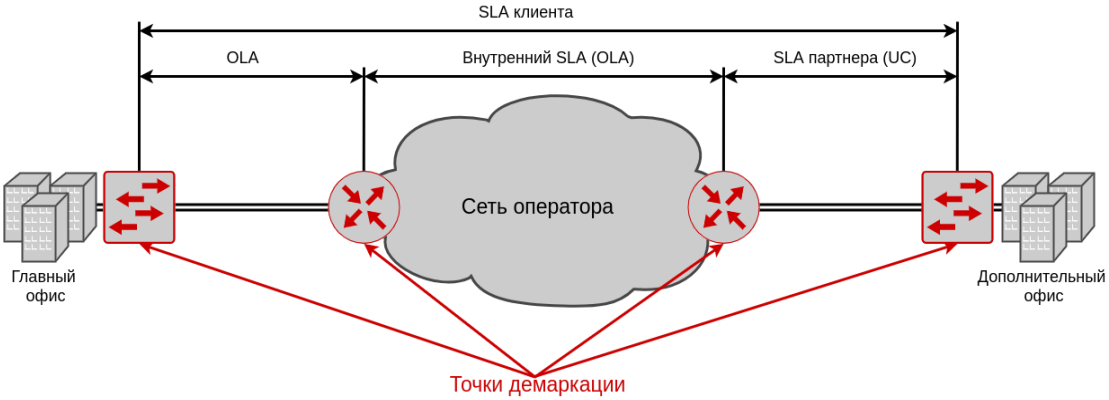


Рис. 6. Варианты точек демаркации [23]

Для разрешения противоречий в точке демаркации, целесообразно использовать измерительные приборы (метрологические средства), т. к. встроенные средства диагностики в этих точках просто не работают. Для разрешения любых конфликтных ситуаций кроме технических средств необходимо еще нормирование этих параметров в рамках SLA-конвенции. SLA позволяет операторам, вне зависимости от действующих стандартов, договориться о параметрах взаимодействия. Один оператор может предложить транзит своего трафика через сеть другого, гарантируя при этом, что параметры передаваемого трафика не изменятся в границах пределов допуска. Например, транзитная сеть не имеет права увеличить количество потерянных вызовов более чем на 5 % из-за своей деятельности и т. д. Если речь идет о новой технологии, для которой еще нет разработанных норм национальных стандартов, и присутствует правовой вакуум, SLA – единственный способ урегулирования взаимоотношений.

При переходе от схемы работы «соответствие/несоответствие национальным стандартам» к SLA качество работы ИТКС в целом не ухудшается, а наоборот, повышается за счет более жестких требований. Гибкость в коммерческой и маркетинговой работе оператора становится необходимым слагаемым успеха. При этом современные системы мониторинга SLA отличаются своей нацеленностью на процессы. В отличие от большинства систем OSS/BSS, они всегда привязаны к особенностям информационного обмена. В основе работы системы мониторинга SLA лежит процесс разрешения конфликтов между поставщиком и потребителем услуг связи на основе управления сквозными процессами ЖЦ услуг (PLM), рис. 7.

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

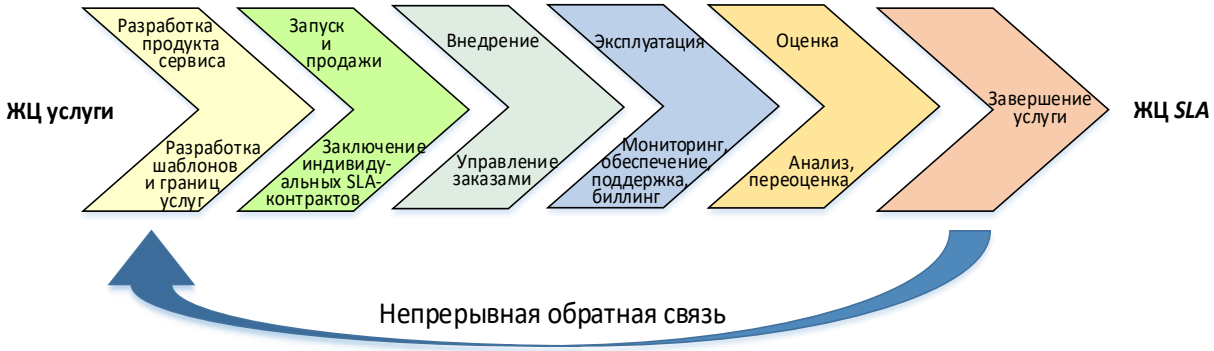


Рис. 7. Сквозной цикл предоставления услуги SLA

Система осуществляет управление не отдельными услугами и метриками, а непосредственно контрактами SLA, что позволяет полностью учитывать в ней организационно-технические процедуры, связанные с управлением SLA (согласование SLA-договора, управление его изменениями и версиями, политикой и стандартами качества компании-оператора). Все это делает системы мониторинга SLA весьма актуальными и значимыми, относя их к классу самых современных. Ориентированность на обеспечение процесса повышает результативность этих систем, что в сочетании с оперативностью развёртывания и технологичностью, усиливает эффективность данного класса систем на рынке.

В отличии от систем OSS, системы мониторинга SLA позволяют быстро установить полный контроль состояния отдельного сегмента или всей сети в целом, поскольку они вообще не вмешиваются в оборудование (не позволяют управлять), а только контролируют состояние. При этом SLA позволяет учесть особенности и измерить любую сеть или ее отдельные сегменты.

Также важно отметить, что только режим реального времени для сетевого мониторинга поможет иметь телеком-оператору объективную картину метрик SRE для различных потребителей и их доступа к приложениям ИТКС. При этом, если в SLA-договоре оговариваются лишь отношения с внешним потребителем услуг, то SRE-метрики необходимы в большей степени самому оператору для выработки общей ответственности его технического персонала и SRE-инженеров за доступ к приложению (сервису) при функционировании ИТКС. Лишь постоянный мониторинг качественных параметров ИТКС в совокупности с общей системой управления, сбора и обработки измерительной информации (ИИ) реального времени дают объективную картину поддержания функциональной безопасности ИТКС в плане обеспечения доступа к их приложениям.

Важно отметить, что все приложения условно могут быть разделены на две основные группы: приложения, при неудовлетворительной работе которых может наступить уголовная ответственность пользователя (критически важные приложения); приложения, использование которых при низком качестве сетевых услуг несет финансовые и репутационные потери пользователя [21]. В этих случаях SRE-метрики могут лечь в основу судебных претензий к телеком-оператору, как поставщику услуг при включении в SLA-договор их качества.

Таким образом, сетевой мониторинг в SRE-метриках на сегодня является единственным объективным и надежным методом (технологией) оценки пара-

метров эффективного функционирования ИТКС, что требует разработки и совершенствования SRE-инструментария.

Существует множество и других решений, работающих поверх общедоступных и частных облаков, которые отслеживают использование облачных ресурсов. Среди них можно отметить следующие:

– ***Amazon CloudWatch*** [26] – это служба мониторинга и управления, отслеживающая виртуальные ресурсы пользователей, такие как экземпляры виртуальных машин Amazon EC2;
– ***GMonE*** [27] – универсальный инструмент облачного мониторинга, предлагающий унифицированную таксономию, на основе чего определяется его многоуровневая архитектура;
– ***PCMONS*** [28] – система мониторинга частного облака, которую можно адаптировать для использования поставщиками облачной телефонии для сбора и централизации информации;
– ***IBM Tivoli Monitoring*** [29] наряду с OSS и другими системами мониторинга [30] также направлена на оптимизацию производительности и доступности ИТ-инфраструктур за счет сосредоточения внимания на физических ресурсах;
– ***MonPaaS*** [31] – платформа адаптивного мониторинга с открытым исходным кодом как услуги. Она объединяет Nagios [14] и OpenStack. MonPaas отслеживает физические и виртуальные ресурсы, а также обновляет любые изменения в физической или виртуальной инфраструктуре. Недостаток – потребляет дополнительные физические ресурсы.

Место систем мониторинга в обобщенной архитектуре управления ИТКС приведено в таблице 3 с представлением вышерассмотренных систем относительно реализации модели функциональной безопасности сети (*FCAPS*):

– (F) Fault Management / Управление отказами;
– (C) Configuration Management / Управление конфигурацией;
– (A) Accounting Management / Учёт;
– (P) Performance Management / Управление производительностью;
– (S) Security Management / Управление безопасностью.

Таким образом, в соответствие с анализом функций управления ИТКС (таблица 3) можно сделать следующие выводы:

– на мониторинг устройств ориентированы такие из рассмотренных систем как Zabbix, Nagios, Cacti, Prometheus, OpenNMS и HP Open View;
– для мониторинга соединений и мониторинга сетей предназначены Zabbix, Nagios, Cacti, OpenNMS и HP Open View;
– осуществлять мониторинг сервисов могут практически все из перечисленных систем мониторинга.

Таблица 3 – Место систем мониторинга в обобщенной модели управления ИТКС ОП

Системы мониторинга	Функции модели управления информационно-телекоммуникационными сетями (**F-C-A-P-S**)					Функции системы мониторинга			
	(**F**) Fault Management /Управление отказами	(**C**) Configuration Management / Управление конфигурацией	(**A**) Accounting Management / Учёт	(**P**) Performance Management / Управление производительностью	(**S**) Security Management / Управление безопасностью	Мониторинг устройств	Мониторинг соединений	Мониторинг сетей	Мониторинг сервисов
System Center Operations Manager (SCOM)	+/– (монито-ринг сервисов)	+ (управление конфигурацией сервисов)	+ (учет сервисов)	+	+	–	–	–	+
Zabbix	+	+/– (только устройства и сервисы)	+	+	–	+	+/– (отсутствует понятие канала)	+/– (RMON)	+
Nagios (Linux)	+	–	+/–	+	–	+	+/– (отсутствует понятие канала)	+/– (RMON)	+
Cacti	– (только сбор данных)	–	+ (без обработки)	+	–	+	+/–	+/– (RMON)	+
Prometheus	+	–	+	+	–	+	–	–	+
OpenNMS	+	+	+	+	–	+	+/–	+/– (RMON)	–
Amazon CloudWatch	+	–	+	+	–	–	–	–	+
GMonE	+	–	+	+	–	–	–	–	+
PCMONS	+	–	+	+	–	–	–	–	+
IBM Tivoli Monitoring, HP Open View	+	+	+	+	–	+	+/–	+	+
MonPaaS	+	+	+	+	–	–	–	–	+

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

4. Функции подсистем мониторинга информационно-телекоммуникационной сети общего пользования

Изначально на ИТКС ОП функции мониторинга осуществляли администраторы, а информация о ТС систем в лучшем случае собиралась ими же в каких-либо неспециализированных программах (по причине их отсутствия), в худшем же вообще никак не накапливалась и не агрегировалась. Сведения об эксплуатируемом объекте контроля (ОК) были привязаны к практическому опыту работы конкретного специалиста с сетевой инфраструктурой и полностью терялись при его увольнении. В настоящее же время практически любая система мониторинга реализует модель FCAPS [32]. Появилось множество полу- и полностью автоматизированных систем мониторинга, анализирующих ТС сетевых элементов и отдельных сетей ИТКС, осуществляющих сбор ИИ по контролируемым параметрам и вероятностно-временным характеристикам во временные ряды, удобные для визуализации диаграммы, таблицы и графики, которые при необходимости (в случае аномалии) можно анализировать.

Для хранения получаемой в ходе мониторинга ИИ об ОК обычно используется конфигурационная БД под различными системами управления, где информация об объекте контроля представлена, как набор конфигурационных единиц. Каждый сервер и каждое сетевое устройство, подвергаемое мониторингу, представляет собой некую единицу, ИИ о которой хранится в централизованной БД. Такое представление позволяет впоследствии интегрировать подсистему мониторинга с подсистемой визуализации в интересах системы поддержки принятия решений (СППР) на управление ИТКС (АСУС) и др. Ключевым элементом подсистемы сетевого мониторинга является *сервер мониторинга*, который с позиции области применения и наблюдаемого пространства может формироваться различно. Для мониторинга функционального состояния ИТКС предложен следующий вариант его построения, рис. 8.

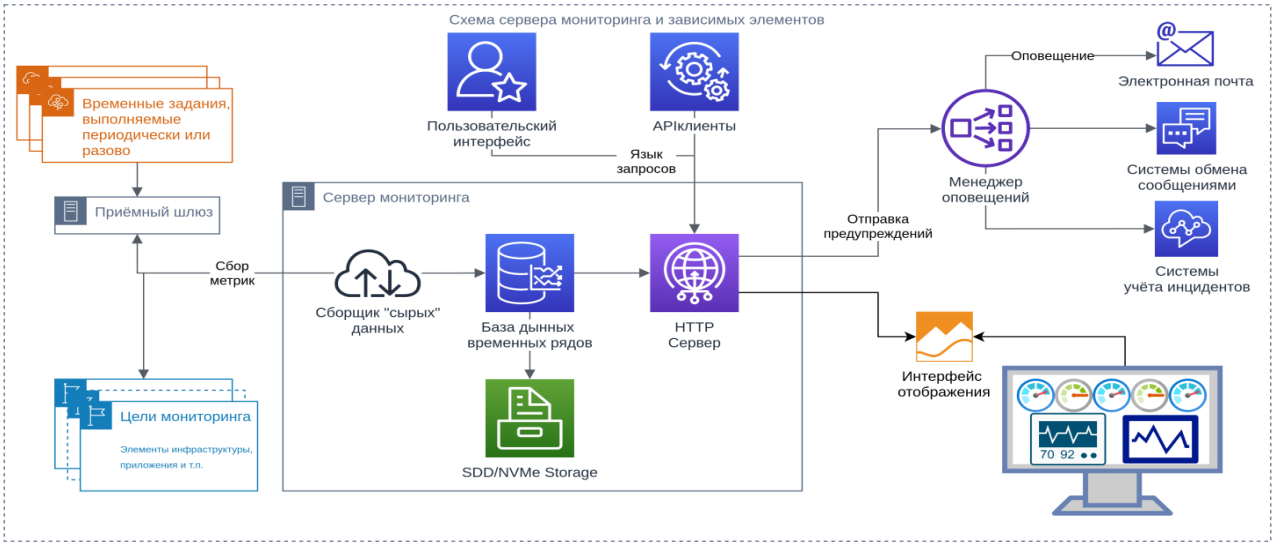


Рис. 8. Структурная схема сервера мониторинга ИТКС и зависимых элементов (вариант)

Структурно сервер мониторинга [20] состоит из сборщика сырых данных, базы данных временных рядов и HTTP или SNMP сервера, функционирующих во взаимодействии с объектами мониторинга, подсистемой оповещения и подсистемой отображения. Сборщик сырых данных опрашивает объекты мониторинга по протоколу HTTP или SNMP и помещает собранные метрики в базу данных временных рядов. В базе данных хранятся метрики мониторинга одного и того же объекта на протяжении заданного времени наблюдений. Таким образом, возможно определение изменений значений параметров ОК во времени.

Информационная архитектура современных систем мониторинга исходит из реализации функциональной модели FCAPS [32], 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).

Основные задачи указанных функциональных проекций в части мониторинга приведены в таблице 4.

Таблица 4 – Задачи мониторинга согласно модели FCAPS

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

В общем случае процесс мониторинга сети включает следующие этапы [19]:
- 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.

После первоначального развертывания системы мониторинга производится анализ структуры сети, т. е. запись в базу данных системы требуемой информации о топологических отношениях между сетевыми элементами – устройствами, каналами, интерфейсами. На последующих 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 является компонент диспетчеризации событий, совмещенный с настраиваемым классификатором событий, отказов и предупреждений (соответственно рекомендаций M.3703 [12]). В случае OpenNMS таким компонентом является процесс-диспетчер событий EventD, OpenView – процесс PMD, U2000LCT – MRB.

Сервисы системы мониторинга, подключаемые к диспетчеру событий, строятся по рассмотренным проекциям управления: отказами, конфигурацией, учетом, производительностью, безопасностью. В части мониторинга конфигурации это компонент анализа структуры сети (ovtopmd в HPOpenView, discovery в OpenNMS, Discovery Service в U2000LCT).

Мониторинг производительности реализуется компонентами сбора данных и SNMP-извещений (OpenNMS – collectd и trapd, HPOView – snmpcollect и ovtrapd, U2000LCT – NEDataCollector).

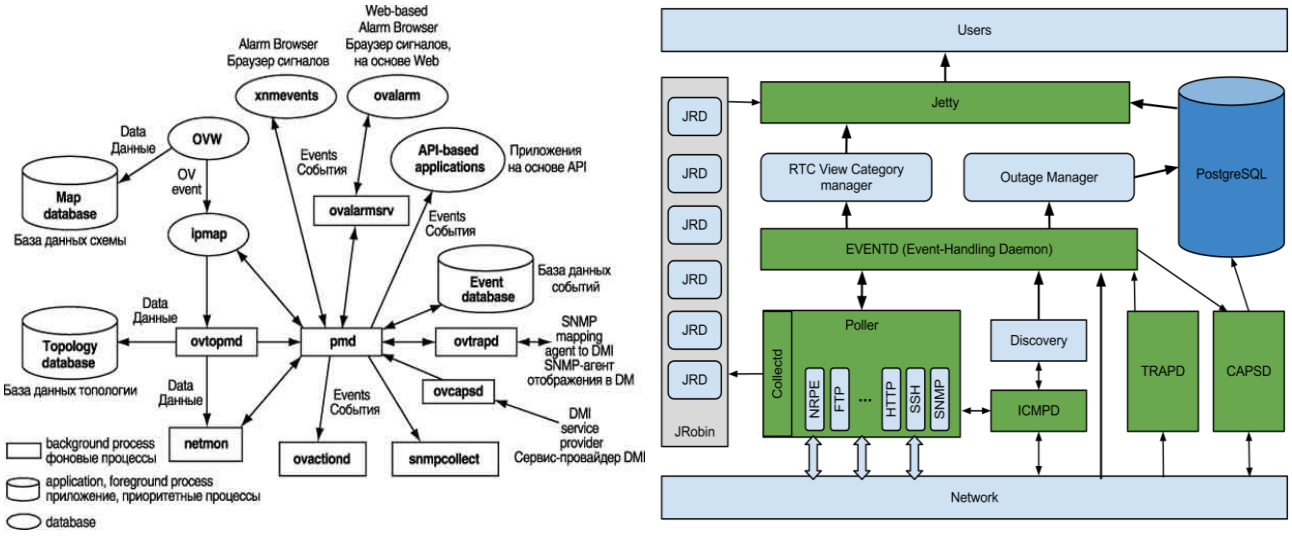
Мониторинг ресурсов реализуется компонентами тестирования высокоуровневых сервисов (HP OpenView – ovcapsd, OpenNMS – capsd и poller).

Управление отказами также реализуется компонентами работы с отказами (HP OpenView – ovalarm, OpenNMS – outaged).

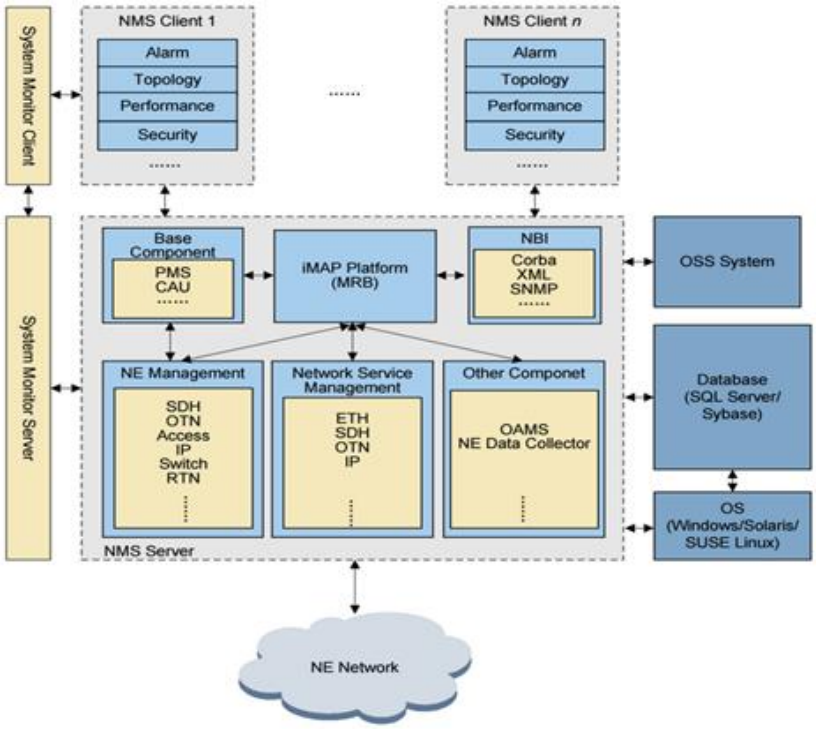
Обобщенная архитектура системы мониторинга представлена на рис. 9.

В случае OpenNMS таким компонентом является процесс-диспетчер событий EventD, OpenView – процесс PMD, U2000LCT – MRB.

Сервисы OSS, подключаемые к диспетчеру событий, строятся по проекциям управления: отказами, конфигурацией, учетом, производительностью, безопасностью.



a) *b*)



c)

Рис. 9. Интеграция высокоуровневых архитектур
за счет компонента-диспетчера классифицированных событий:
a) Hewlett-Packard NNM [33], *b*) OpenNMS, *c*) U2000LCT Huawei [34]

Можно также выделить:

– компонент анализа структуры сети (ovtopmd в HP OpenView, discovery в OpenNMS, Discovery Service в U2000LCT);
– компоненты сбора данных и SNMP-трапов (OpenNMS – collectd и trapd, HPOView – snmpcollect и ovtrapd, U2000LCT – NEDataCollector);
– компоненты тестирования высокоуровневых сервисов (HP OpenView – ovcapsd, OpenNMS – capsd и poller);
– компонент работы с отказами (HP OpenView – ovalarm, OpenNMS – outaged).

В обобщенной архитектуре системы мониторинга четко выделяется 3-уровневая схема обработки, которая полностью согласуется с рекомендацией М. 3703 [12]:

– события (events), получаемые после обработки процессами сбора первичных данных при сравнении измерения с пороговым значением, или посредством выявления фактов в анализируемых журналах (аудита);
– данные, получаемые посредством измерений;
– отказы (faults) и предупреждения (alarms), получаемые в результате логического вывода на множестве событий (events).

Например, событие, свидетельствующее о переходе устройства из работоспособного состояния в неработоспособное состояние, считается отказом, в то время как переход из неработоспособного в работоспособное, очевидно, нет.

В процессе обработки наблюдается уменьшение объема данных при переходе от данных к событиям и от событий к отказам. Данная процедура перехода регламентируется классификатором событий, который строится на основе рекомендаций М.3703 (см. [12]).

Обобщенный формат передаваемых диспетчером событий в упрощенном виде показан на рис. 10.

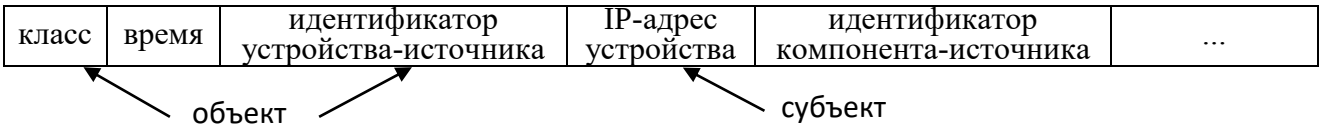


Рис. 10. Упрощенный формат события системы мониторинга. Поля, относящиеся к логике коммутации событий

В случае OpenNMS таким компонентом является процесс-диспетчер событий EventD, OpenView – процесс PMD, U2000LCT – MRB. Сервисы OSS, подключаемые к диспетчеру событий, строятся по проекциям управления: отказами, конфигурацией, учетом, производительностью, безопасностью. Можно также выделить: компонент анализа структуры сети (ovtopmd в HP OpenView, discovery в OpenNMS, Discovery Service в U2000LCT), компоненты сбора данных и SNMP-трапов (OpenNMS – collectd и trapd, HPOView – snmpcollect и ovtrapd, U2000LCT – NEDataCollector), компоненты тестирования высокоуровневых сервисов (HP OpenView – ovcapsd, OpenNMS – capsd и poller), компонент работы с отказами (HP OpenView – ovalarm, OpenNMS – outaged).

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», рис. 11 [14], т. е. в процессе обработки событий субъекты выстраиваются в цепочки. Интеграция событий происходит за счет компонента-диспетчера классифицированных событий. Рассмотрим подробнее работу компонента диспетчеризации [35].

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.

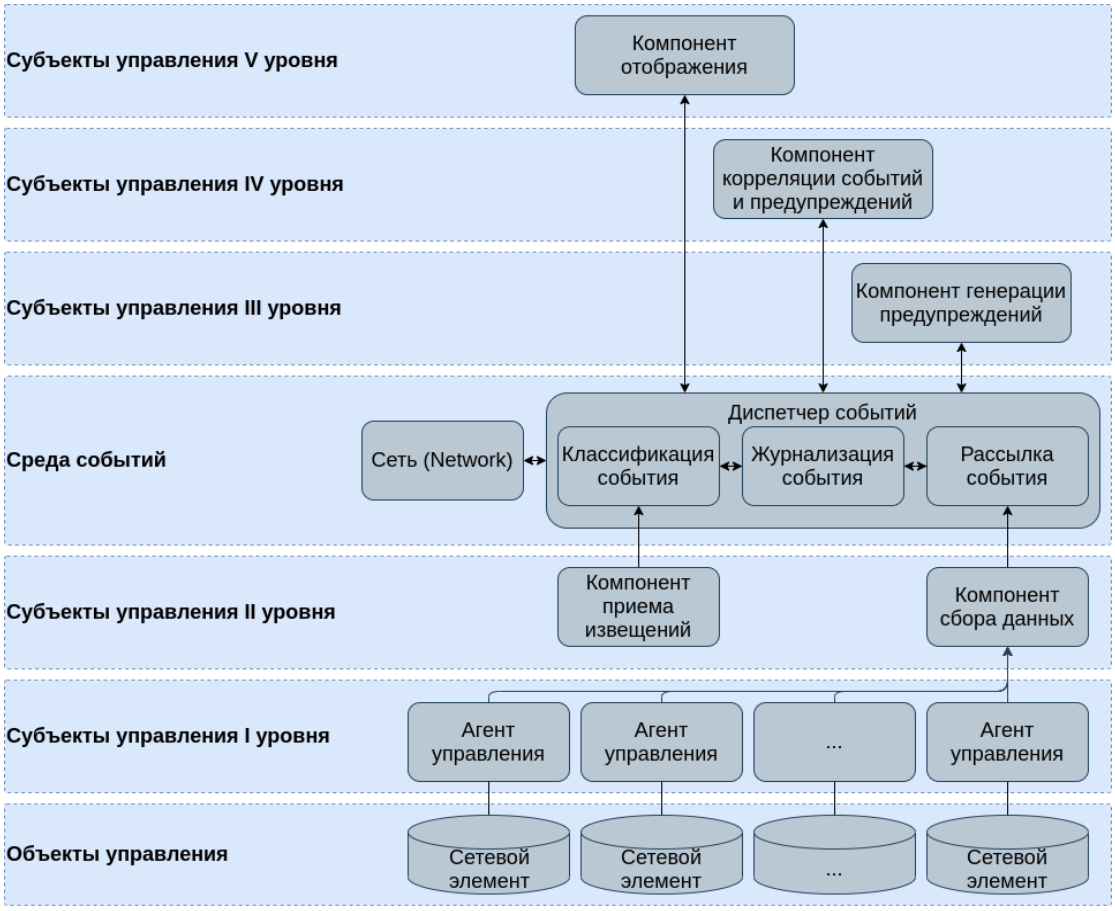


Рис. 11. Обобщенная архитектура системы мониторинга

При поступлении события в компонент диспетчеризации оно обрабатывается цепочкой процессоров:

– процессор классификации и расширения описания события. Классификация событий осуществляется за счет подгрузки из классификаторов дополнительных данных;
– процессор для осуществления записи события в БД;
– 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 проблем (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.

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, что показано на рис. 3, рис. 4. 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. Например, на рис. 3 приведен фрагмент сети, характеризуемой своей картой (с топологией «кольцо»), который отображается в виде знака-символа на карте более высокого уровня. Причем цвет знака характеризует совокупное состояние символов на соответствующей символу суб-карте. Схема вычисления состояния задается оператором при помощи правил агрегации и фильтрации событий.

Таким образом, исходя из вышеуказанного, среди ***основных функций*** существующих систем мониторинга ИТКС 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 ин-

формации ЛПР, при этом возможен выбор для визуализации нескольких 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 систем 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 устройствами (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 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.

5. Методы интеллектуальной обработки данных (значений временных рядов) в современных системах мониторинга

Изменение большого числа контролируемых характеристик ИТКС ОП и ее основных элементов (серверов, узлов коммутации, периферийных устройств, каналов, маршрутов) носит характер случайного процесса, представляемого временными рядами. При этом статистический характер принятия решений о функциональном состоянии сетевого элемента и ИТКС в целом особенно хорошо прослеживается с ростом размерности объекта и увеличением скважности

№4. 2021
ISSN 2410-9916

его опроса серверами мониторинга, что существенно влияет на увеличение количества обрабатываемой измерительной информации сервером мониторинга. А учитывая тот факт, что наблюдение за сетевыми объектами мониторинга осуществляется практически на протяжении всего их ЖЦ, то задачи обработки временных рядов в современных подсистемах мониторинга справедливо относят к задачам анализа больших данных (Big Data).

Временной ряд случайного потока отказов, влияющего на показатели надежностных характеристик сетевых устройств ИТКС, можно представить случайным процессом [36], в основе которого всегда лежит математическая модель. При этом большинство моделей предполагают, что прогнозирование случайного процесса общего вида основано как на аддитивном представлении случайного процесса в виде суммы декомпозиций трендовой, периодической (циклической) и стохастической компонент, так и на мультипликативном их представлении, т. е. произведении данных компонент.

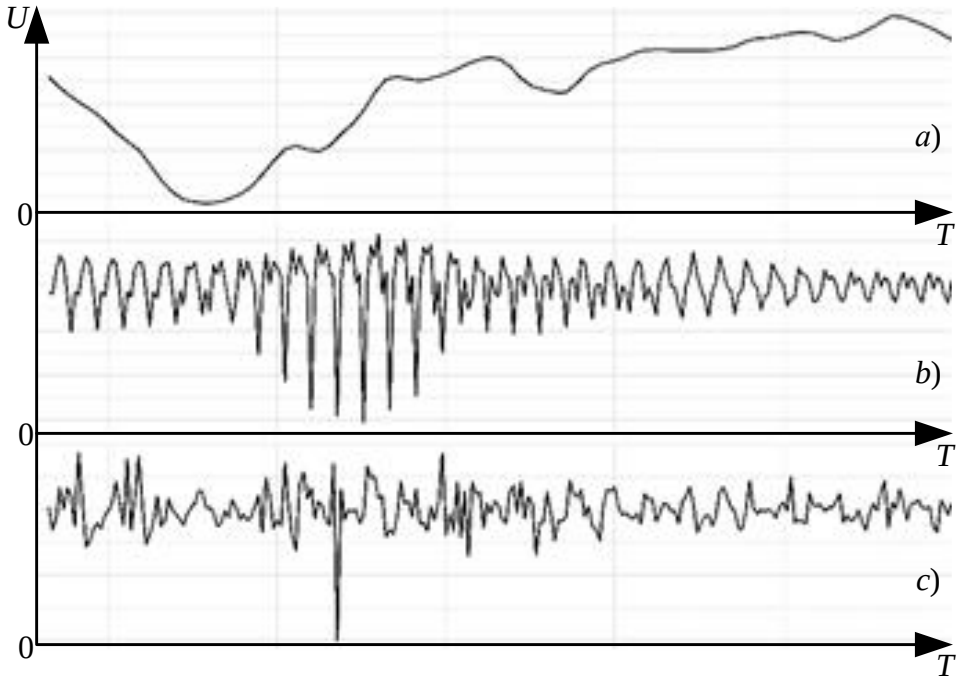


Рис. 12. Основные разновидности случайных процессов, представляемые временными рядами

Рассмотрим указанные компоненты случайного процесса, рис. 12:

– тренд случайного процесса (рис. 12, a) – некоторая детерминированная компонента, не содержащая периодических составляющих, кроме, тех, периоды которых заведомо больше интервала временного окна наблюдения случайного процесса;
– периодическая (циклическая) компонента (рис. 12, b) – определяется как совокупность неслучайных гармонических колебаний, периоды которых заведомо меньше, чем интервал временного окна наблюдения случайного процесса;
– случайная компонента (рис. 12, c) – центрированный случайный процесс.

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

Выбор какой-либо из известных в настоящее время математических моделей прогнозирования и ее применение к компонентам случайного процесса (временным рядам) зависит, прежде всего, от степени статистической значимости каждой из данных компонент (т. е. доли дисперсии компоненты в дисперсии всего процесса), а также степени ее регулярности, поскольку параметры регулярных компонент изменяются сравнительно медленно, при этом закон их изменения известен или возможно получение его достоверной оценки.

Для прогнозирования отказов (предотказного технического состояния [7]) по временным рядам анализируемых метрик сетевых элементов и ИТКС в целом наибольшую статистическую значимость могут иметь регулярные периодические (циклические) компоненты. Это подтверждается теорией надежности, в соответствии с которой отказы элементной компонентной базы (ЭКБ) и состоящих из нее сетевых элементов носит как раз периодический характер, связанный с периодами изменения нагрузки, сезонностью воздействий внешних условий и пр. Трендовая компонента в таких рядах, как правило, является монотонной, имеет постоянные либо сравнительно медленно меняющиеся значения параметров, связанные с деградационными процессами в ЭКБ (рис. 12, а). Трудностей с построением ее модели и прогнозом обычно не возникает. В свою очередь, случайная компонента или имеет малую статистическую значимость, или носит периодический характер, аналогичный сезонной (зависимость от режимов функционирования сетевого элемента или условий эксплуатации). Природа таких временных рядов может быть самой различной. Примерами могут служить всевозможные технологические показатели сети – повышение различных параметров информационного обмена на ИТКС в часы наибольшей нагрузки (ЧНН), изменения загрузки ЦПУ в соответствии с режимами работы сетевых элементов (недогруженный, нагруженный, перегруженный режимы работы), ежедневные объемы услуг отдельных сервисов и многие другие.

В настоящее время наиболее распространенными из моделей и методов, реализуемых в сервере мониторинга и направленных на решение задач прогнозирования поведения временных рядов, содержащих регулярные периодические компоненты являются следующие.

Метод Винтерса или обобщенный метод экспоненциального сглаживания [37], заключающийся в способности реализовать обычную фильтрацию с экспоненциально затухающей импульсной переходной функцией. При этом учет периодической компоненты в ходе прогноза обеспечивают путем взятия через интервал периодичности значений прогнозируемого процесса. В то же время, этот подход, учитывает лишь закономерности процесса, которые проявляются на интервале периодичности, с характерным методу соответствующим экспоненциальным сглаживанием.

Также при анализе временных рядов широко используется сезонная ***модель авторегрессии проинтегрированного скользящего среднего*** (АРПСС) (auto regressive integrated moving average) [38]. АРПСС уходит от экспоненциального сглаживания, однако, при этом учет периодической компоненты так же, как и в предыдущем методе обеспечивается взятием значений прогнозируемого процесса через интервал периодичности. При этом недостатком данной

модели является то, что ее упрощение за счет ограничения порядка авторегрессии и скользящего среднего значительно снижает качество прогноза для случаев, когда прогнозируемый процесс имеет сложные корреляционные связи.

Метод сингулярного спектрального анализа [39] изначально предполагает значительную зависимость от решений, принимаемых на каждом его этапе, в частности, от выбора параметров (длины окна анализа, числа компонент), способа группировки компонент, алгоритма восстановления ряда. Это требует крайне высокого уровня компетенций эксперта, адаптирующего данный метод для решения конкретной задачи, и значительно ограничивает возможности его применения.

Топологические методы анализа временных рядов. В последнее время для выявления закономерностей и поиска аномалий в сложных данных больших объемов (Big Data) существенное развитие также получили топологические методы анализа TDA (Topology Date Analysis) [40]. Такой подход предполагает, что в качестве исходных данных при построении и сравнении базового и текущего профиля используются облака данных как неупорядоченные наборы данных, не привязанные к какой-либо из шкал измерений, например, временной. При этом облако данных (множество X принадлежит евклидову пространству размерности d: $X \subset R^d$) представляют в виде множества точек в заданном топологическом пространстве (например, пространстве метрик сетевых элементов ИТКС), к которому применимы процедуры *TDA*. А поскольку в данном методе исходные данные в основном представлены временными рядами, то временной ряд преобразуется без потери информации в облако точек, рис. 13, где каждому элементу в облаке данных ставится в соответствие точка в соответствующем облаке.

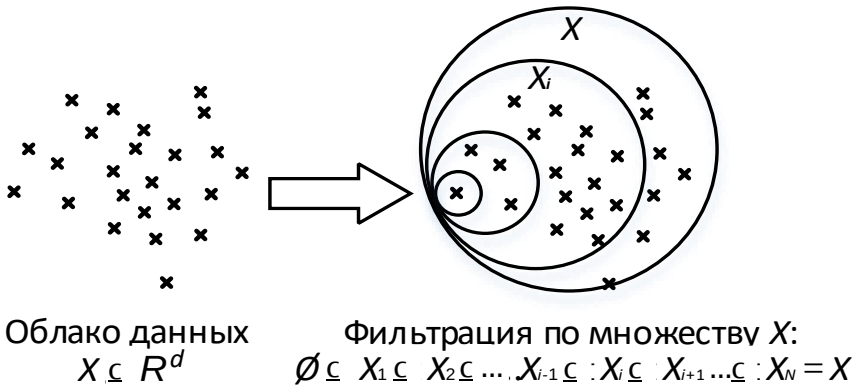


Рис. 13. Общая схема TDA

При этом на первом этапе метода временные ряды, описывающие во времени изменяющееся поведение пользователя или иной сущности, преобразуются в облако точек топологического пространства без потери информации (с использованием методического аппарата теории вложения Такенса-Мане [41] или алгоритма ложных соседей [42]). На этом этапе подбирают такое топологическое пространство, элементами (точками) которого и будут элементы временных рядов. На следующем этапе, после определения топологического пространства (с входящим в него облаком точек) возможно вычисление топологи-

ческих инвариантов, а также их производных характеристик в интересах выявления особенностей анализируемого временного ряда. Далее, для текущего (актуального по времени измерения) и базового (эталонного) облаков точек строятся топологические зависимости (диаграммы, графики и пр.), характеризующие текущий и базовый профили поведения соответственно. На завершающем этапе, с использованием алгоритма шкалирования на основе обобщенной функции желательности Харрингтона [43], метрик Вассерштейна [44], Чебышева [40] и других методов, выявляют отклонения текущего (наблюдаемого) от базового профиля поведения.

В последнее время для прогнозирования временных рядов также широко используются ***нейросетевые алгоритмы*** [45-48]. С учетом специфики разнородности сетевых устройств на распределенных ИТКС, задача контроля и прогнозирования их состояния является нелинейной, не поддающейся строгой формализации традиционными математическими методами. В особых условиях функционирования сетевого оборудования – при воздействии дестабилизирующих факторов внешних (естественной природы), и внутренних (перегруженные режимы работы и сложные условия эксплуатации), когда решение задачи в общем виде невозможно, оправдан нейросетевой подход, позволяющий обеспечить достаточно высокое качество выполнения задачи. Для решения задач аппроксимации нелинейностей важны методики, разрешающие проблемы принятия решений в условиях неполных данных (нехватки априорной, статистической информации) с учетом постоянно изменяющихся условий окружающей среды, что позволяют возможности нейро-технологий.

Искусственная нейронная сеть (ИНС) не требуют традиционного программирования: информация обучения ИНС накапливается в весах, а не в программах, что обеспечивает устойчивость работоспособности сети. К другому достоинству ИНС следует отнести свойство обобщения, то есть способность сети давать правильные ответы на любые входные данные, не относящиеся к обучающему множеству.

На рис. 14 приведен пример построения обобщенной схемы модели контроля технического состояния (ТС) сложных технических объектов [12, 13], в которой объединены две ИНС: самоорганизующаяся карта Кохонена [11] и трехслойная гибридная нейросеть. Для фильтрации полученных на выходах нейросети значений показателей ТС и определения выходного класса ТС, соответствующего текущему ТС сетевого элемента, используются блоки, реализующие ступенчатую функцию с заданным порогом активации.

Функционирование модели предполагает:

– кластеризацию значений показателей;
– обработку полученных значений при помощи нейросети;
– фильтрацию полученных значений и выделение целевого класса, определяющего текущее значение ТС сетевых элементов.

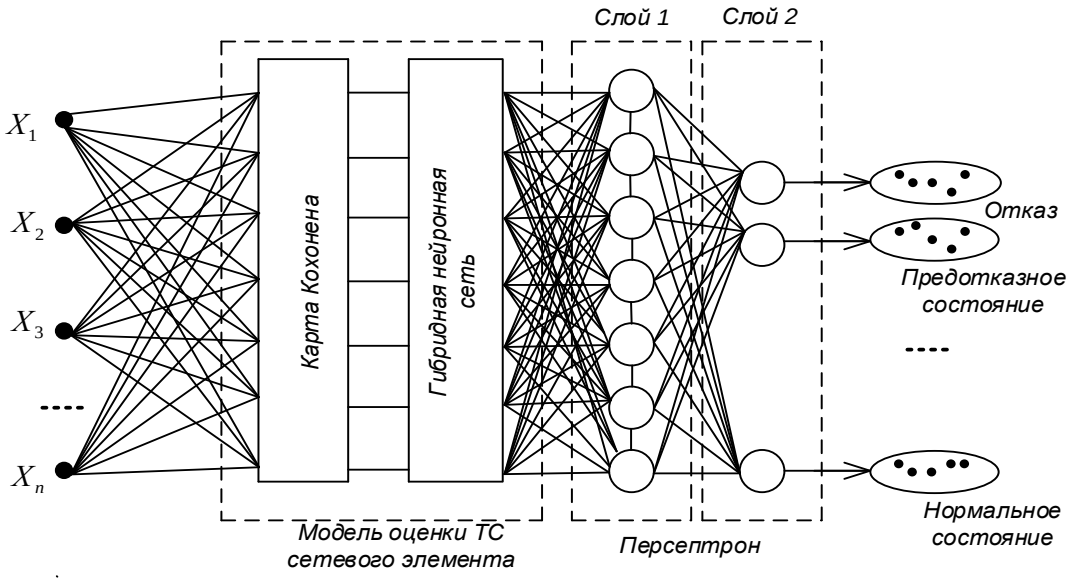


Рис. 14. Модель прогнозирования технического состояния сетевого элемента

Исходя из задач прогнозирования ТС сетевого элемента в [45-47] предложена модель, которая, в отличие от рассмотренной имеет многослойный персептрон, а также использование на выходе модели аппарата дискретного вейвлет-преобразования (ДВП), что характеризует модель относительной простотой структуры и высокой точностью выходных данных.

Персептрон играет в модели роль модуля прогнозирования, который получает на входы результаты работы нейросети, определяющие по совокупности показателей текущее ТС сетевого элемента. Далее он формирует на выходах прогнозные значения, отражающие принадлежность ТС определенному классу состояний через заданный интервал времени. Результаты прогнозирования фильтруются блоками, реализующими фильтрацию полученных значений с использованием ДВП. Тем самым обеспечивается определение одного из результирующих классов ТС, характеризующих прогнозируемое техническое состояние сетевого элемента [46, 47].

Использование метода ***дискретного вейвлет-преобразования***, значительно упрощает процесс решения задачи комплексной прогнозной оценки ТС сетевых элементов, отличающей данный метод от других, включающих задачи объединения методов отбраковки аномальных измерений, фильтрации и сжатия данных, выявления локальных особенностей измерительной информации в интересах прогнозирования аварийных и нештатных ситуаций. Предложенная аппроксимация областей работоспособности эллипсоидами [48] позволяет повысить контрастность классов ТС и получить более гарантированную оценку, рис. 15.

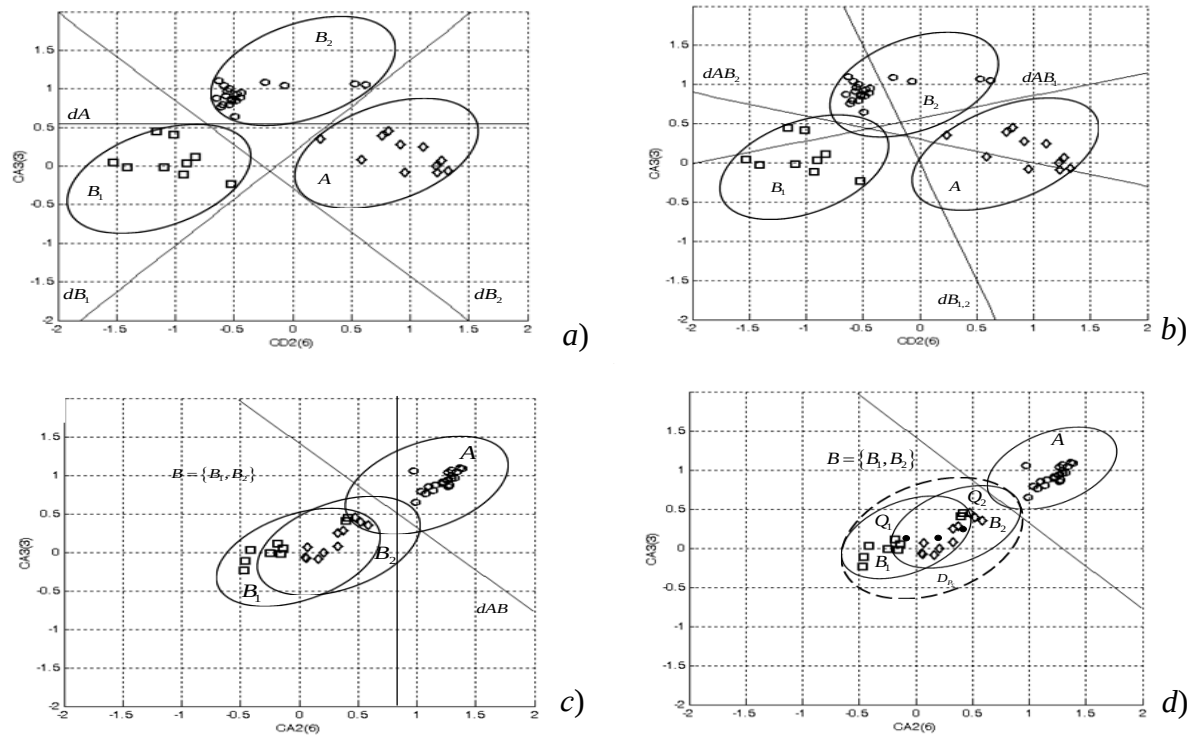


Рис. 15. Применение ДВП для разделения классов ТС в виде областей работоспособности [48]: *a*) неперекрывающихся; *b*) частично перекрывающихся, *c*) перекрывающихся; *d*) объединенных (на рис. обозначены: A – работоспособное, B_1 – неработоспособное, B_2 – предотказное ТС)

Достаточно активно при исследовании прогнозирования временных рядов на сегодня используется подход ***кластерного анализа*** [49, 50], при котором объектом исследования выступают временные ряды, получаемые от различных источников (распределенный мониторинг технологии «Индустрия 4.0», интернет вещей, «умный город», «умный дом»).

Применяя метод кластерного анализа к объекту исследования в виде подсистемы мониторинга ИТКС ОП осуществляется сбор временных рядов подконтрольных метрик наблюдаемого сетевого элемента, получаемых одновременно с нескольких серверов мониторинга (децентрализованный мониторинг) [51]. При этом за счет использования технологии CRDT (Conflict-Free Replicated Data Type) данные временных рядов с разных серверов мониторинга о наблюдаемом сетевом элементе реплицируются на другие сервера мониторинга подсистемы и обновляются параллельно без координации между узлами. Кластеризационное пространство на каждом сервере мониторинга формируется на основе обобщенных универсальных характеристик временных рядов [52], являющихся координатами этого пространства, в котором значению метрики временного ряда в конкретный момент времени соответствует точка в координатах универсальных характеристик. Фактически объектом анализа является множество временных рядов, порожденных разными серверами мониторинга (источниками) при наблюдении одного сетевого элемента.

На следующем этапе кластерного анализа осуществляется выделение кластеров, элементами которых являются временные ряды одной и той же метри-

ки, наблюдаемые разными серверами мониторинга (близкие в смысле выбранной метрики) и входящими в общее облако данных кластерного пространства. Для каждого из полученных кластеров может быть решена задача о назначении методов прогнозирования, что, в целом, будет способствовать повышению точности прогнозов (за счет выбора метода, который учитывал бы специфику временных рядов, принадлежащих данному кластеру).

Системы поведенческой аналитики. В современной отрасли информационных технологий в последние годы проявляется настойчивый интерес к системам поведенческой аналитики UEBA (User and Entity Behavior Analytics), как к новому классу оценки функциональной безопасности корпоративных ИТКС, основанных на интеллектуальной обработке данных, поступающих в реальном масштабе времени от учетных записей пользователей, а также множества сетевых устройств и приложений [53].

В системах поведенческой аналитики [54] предполагается, что сервер мониторинга получает информацию от источников D подсистем встроенного контроля сетевых элементов $D = \{d_n | n = \overline{1, N}\}$. От каждого датчика или сенсора сетевого устройства поступают кортежи поведенческих характеристик H (временные ряды) $H = \{h_m | m = \overline{1, M}\}$, свойственные каждому сетевому элементу технологии «Индустрия 4.0» или классу объектов мониторинга O_n: $H_1(O_1) = \langle h_{11}, h_{12}, ..., h_{1m} \rangle$; $H_2(O_2) = \langle h_{21}, h_{22}, ..., h_{2m} \rangle$; …; $H_n(O_n) = \langle h_{n1}, h_{12}, ..., h_{nm} \rangle$, и которые определяют реализацию дальнейших действий. В качестве характеристик могут рассматриваться как внешние, так и внутренние признаки, позволяющие проводить анализ текущего состояния объекта мониторинга, и по аномальным отклонениям одной метрики идентифицировать изменения в поведении временного ряда другого параметра (рис. 16). К ним можно отнести численные данные, интервальные данные, ранговые данные, номинальные данные. При этом текущее состояние системы описывают функциональной сетью Z, которая идентифицирует от источников набор кортежей $Z = \{h_l | l = \overline{1, K}\}$, где K – число функциональных состояний сетевого элемента, которые необходимо проанализировать для выявления аномалии.

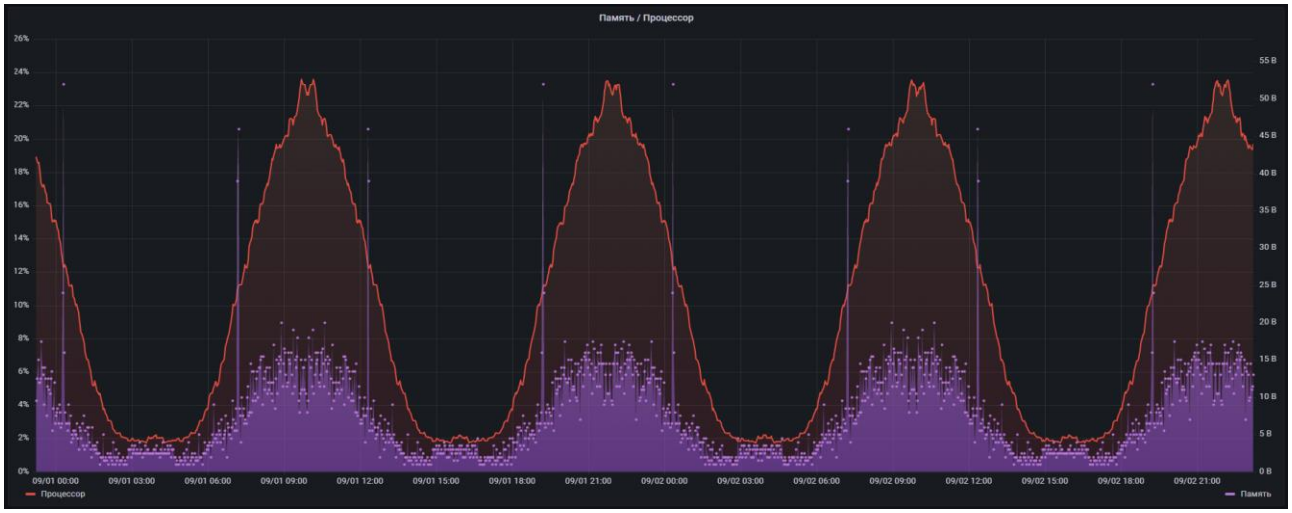


Рис. 16. График изменения загрузки процессора (красн. цв.) и памяти (син. цв.)

Тогда на основе поведенческого подхода [54] задача определения технического состояния сетевого элемента ставится следующим образом.

Пусть C – множество классов состояний, характеризуемое в соответствие с [7] как «исправное», «работоспособное», «предотказное», «предельное» и т. д., или в соответствии с [12] – как «неопределенное» (Undefined, *U*), «норма» (Normal, *N*), «незначительное нарушение» (Minor, *I*), «значительное нарушение» (Major, *J*), «критическое» (Critical, *C*), «авария» (Fault, *F*). Выбрана функция расстояния между объектами $r(z, z`)$. Имеется конечная обучающая выборка заданных технических состояний $Z^k = \{z_1, z_2, \ldots, z_m\} \in Z$. Необходимо разбить данную выборку на подмножества, которые бы включали технические состояния, близкие по метрике r, т. е. найти функцию a: $Z \rightarrow C$. В конечном итоге в ходе анализа на основе функциональной сети Z определяют текущее состояние («нормальное» или «аномальное») исходя из особенностей классических способов анализа – байессовского, наивного байессовского, нейросетевого и др.

При решении подобных задач на распределенных ИТКС у исследователя возникает необходимость анализа состояния не только сетевых устройств, но также сопрягающих их каналов и протекающих процессов. При этом в большинстве случаев внутренние состояния удаленных (автономных) сетевых элементов и процессов, протекающих в них, недоступны для оценки, что требует проведения подобного анализа лишь на основе проявления внешних характеристик сетевого элемента в системе (ее поведения в сети по отношению к другим сетевым элементам). С этой точки зрения поведенческая аналитика сетевого элемента на основе поступающей измерительной информации по внешним побочным каналам от нескольких других устройств (серверов), сопряженных с ним, является актуальным направлением. Характерная особенность UEBA состоит в построении базового профиля (модели типового поведения) пользователя или иной сущности в виде сетевого устройства. При определенном отклонении пользователя/сущности от базового профиля (установленного шаблона поведения, допусков на эксплуатационные параметры) UEBA регистрирует нарушение (аномалию). Такой подход наиболее применим для систем информационной безопасности [55]. Однако, учитывая, что в области функциональной безопасности процесс обеспечения надежности технических характеристик сложных ИТКС также зависит от пользователя (эксплуатанта) и технического состояния сетевых элементов, то возможно технологию UEBA перенести на область функциональной безопасности [54].

***OLAP* (*online analytical processing*)** – это интерактивная аналитическая обработка данных [56]. В *IT*-системах данные анализируемых временных рядов метрик одного сетевого элемента могут храниться (как правило, хранятся) в разных источниках (на разных серверах мониторинга), а следовательно, это несвязанные между собой базы данных, хранилища событий, файлы, быстрые хранилища, системы статистики. В этом массиве измерительной информации скрывается то, что важно знать системным администраторам, DevOps- и SRE-инженерам для эффективного управления ИТКС и ее услугами. Однако собрать нужные сведения из столь разнородной распределенной структуры и предста-

вить их в виде, удобном для оценки функциональной безопасности сети – проблематично. Термин OLAP был предложен Эдгардом Коддом еще в 1993 году. Им же были сформулированы основополагающие «12 правил аналитической обработки в реальном времени». Предложенная модель OLAP ориентирована на подготовку отчетов, выполнение статистических расчетов на основе анализа больших данных (Big Data), имеющих сложную структуру, а также на построение прогностических сценариев.

OLAP-системы включают следующие основные компоненты:

– базу данных (БД), представляющую собой источник, из которого берется информационный материал для обработки. Тип БД определяется разновидностью OLAP-системы и порядком выполнения действий OLAP сервера. Чаще всего пользуются реляционными и многомерными БД и хранилища данных;
– OLAP-сервер – это ядро системы, с помощью которой ведется обработка многомерных данных, и обеспечивается связь между БД и пользователями системы;
– приложения для работы пользователей, в которых формируются запросы и визуализируются полученные из OLAP-системы ответы.

Особенности обработки данных OLAP-системами состоят в построении многомерных массивов информации, имеющих большое число связей между отдельными элементами. Для формирования этих массивов OLAP-система собирает данные из разных источников. В распределенных децентрализованных системах мониторинга такими источниками могут служить, например, несколько серверов мониторинга, осуществляющих наблюдение за одним сетевым элементом, а также хранилища данных из иных информационных систем управления сетью (АСУС) и пр. После этого информация обрабатывается на OLAP-сервере и передается в пользовательские приложения. При этом хранение и обработка данных с применением OLAP-систем осуществляются как на обособленных серверах в форме многомерных БД, так и непосредственно на рабочих местах пользователей, а также в форме реляционных БД – при совместной работе OLAP-систем с SRE-системами и другими системами мониторинга.

В зависимости от технологий обработки и хранения измерительной информации в БД OLAP-системы классифицируют на несколько видов:

– системы ROLAP, функционирующие с реляционными базами данных (relation – «отношение, зависимость, связь»), где данные сгруппированы в форме таблиц с возможностью аналитики информации в виде чисел и текстов;
– системы MOLAP – многомерные системы, где данные при обработке структурируются в OLAP-кубы на специализированных OLAP-серверах;
– системы HOLAP – «смешанные» системы, где объединены алгоритмы многомерной структуризации данных в форме кубов с размещением их в реляционных таблицах.

В многомерных системах (MOLAP) измерительная информация (данные) об одном сетевом устройстве (элементе) представляется n-мерным кубом, в ко-

тором по осям будут отслеживаемые параметры, а на их пересечении находятся данные. Например, по одной оси могут откладываться временные ряды, относящиеся к функционированию процессора, по другой – характеризующие загрузку памяти, по третьей – интерфейса и т. д. Пользователи могут выбирать нужные в заданное время параметры и получать ИИ по разным измерениям Порядок формирования трехмерного MOLAP-куба метрик сетевого устройства, как со стороны внутренней системы контроля, так и децентрализованной системы мониторинга ИТКС, когда устройство наблюдается несколькими серверами мониторинга, приведен на рис. 17.

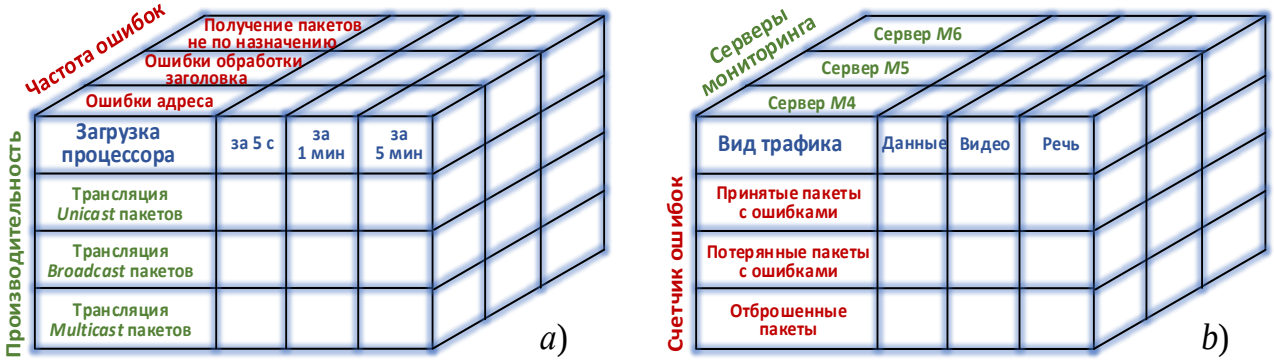


Рис. 17. Порядок формирования трехмерного MOLAP-куба метрик одного сетевого устройства: *a*) его внутренней системой контроля;
b) децентрализованной системой мониторинга ИТКС

При необходимости выполняется «срез» и агрегация статистики изменения измерительной информации одного сетевого устройства (пути, маршрута, канала) на заданном интервале времени и появляется возможность одновременной визуализации наиболее важных метрики как в заданный момент времени, так и в предыдущий временной интервал. Что позволяет OLAP: выявлять причинно-следственные связи между разными метриками, строить гипотезы, моделировать поведение системы при изменениях функциональной безопасности сетевой инфраструктуры, диагностировать причины отказов и прогнозировать развитие аварийной ситуации.

В российском научном сообществе построением многомерных кубов данных систем мониторинга с представлением сети как единого целого одними из первых занимались в научной школе профессора Шерстюка Ю.М. [57, 58].

6. Влияние закона распределения параметров временного ряда на прогнозирование отказа

При анализе методов обработки временных рядов нужно помнить, что основным правилом, определяющим выбор конкретного математического аппарата для их анализа при контроле параметров сетевого оборудования, является степень неоднородности объектов мониторинга [45]. В [59] такая степень неоднородности определяется по шкале (например, от 0 до 1, в сторону увеличения неоднородности). Наиболее подходящий математический аппарат, в зависимости от степени неоднородности, определяется, например, методом экс-

пертных оценок (в частности, метод бинарных сравнений). В целом обоснование степени важности сетевого элемента в распределенной сети определяется на основе положений теории важности критериев:

– *для однотипных сетевых элементов* степень неоднородности ограничена значениями от 0 до 0,6. Это объясняется высокой степенью унификации, «схожести» контролируемых сетевых элементов, а также фиксируемым потоком измерительной информации, характеризуемым свойствами однородности. Процесс изменения ТС в однотипных сетевых элементах более плавный, что способствует относительно высокой эффективности процессов обучения и обобщения, например, при использовании искусственных нейронных сетей. Здесь процедура оценивания ТС основана на методах экспертных оценок, статистических методах распознавания, метрических методах, методах статистических решений (Неймана-Пирсона, минимакса), а также ИНС [45, 59];
– *для неоднотипных сетевых элементов* (например, периферийного оборудования), отличающихся импульсным, нестационарным характером потока измерительной информации с пуассоновским законом распределения или законом распределения Вейбула («рваный» сигнал, получаемый с большим разбросом), поступающего от объекта мониторинга (при степени неоднородности от 0,7 до 1), наиболее применим метод дискретных вейвлет-преобразований, а также метод последовательного анализа Вальда [45, 59].

Для моделирования односторонней задержки каналов связи используются следующие распределения вероятностей непрерывных случайных величин [60]:

– *Гамма-распределение*. Гамма-распределение асимметрично и определено только для неотрицательных действительных чисел. Оно использует два параметра: параметр формы $\alpha > 0$ и параметр масштаба $\beta > 0$. Варьирование α изменяет форму функции плотности, в то время как варьирование β соответствует изменению единиц измерения (например, от микросекунд до миллисекунд) при неизменной форме функции плотности. Исследования показали [61], что гамма-распределение во многих ситуациях адекватно приближает задержки маршрутизации.
– *Распределение Рэлея.* Распределение Рэлея является простой альтернативой гамма-распределению, которое принимает только один параметр – дисперсию σ^2. Эта потеря в степени свободы оправдано тем, что рэлеевское распределение по-прежнему показывает аналогичное поведение во многих случаях хотя является довольно грубым приближением к реальному поведению задержки маршрутизации. Основное преимущество его использования состоит в меньшей вычислительной сложности определения параметра.
– *Смещенное гамма-распределение*. Как только оценены параметры гамма-распределения, моделирующего задержку маршрутизации, можно промоделировать поведение полной задержки, включающей также внутреннюю задержку (передачи пакетов по физической среде) *c*. Для этого гамма-распределение должно быть дополнено третьим парамет-

ром $c > 0$, которая сдвигает пик распределение на c единиц вправо. Это линейное преобразование приводит к распределению, называемому смещенным гамма-распределением. Внутренняя задержка c независима от состояния маршрутизаторов на пути, которые, в свою очередь, моделируется посредством параметров α и β.

– *Смещенное распределение Рэлея*. смещенное распределение Рэлея, так же, как смещенное гамма-распределение, является обобщением с дополнительным параметром $c > 0$, учитывающим внутреннюю задержку.

Функции плотности указанных распределений вероятностей вместе с их математическим ожиданием и дисперсией приведены в таблице 5.

Графики функций плотности распределения вероятностей с несколькими выбранными параметрами представлены в таблице 6.

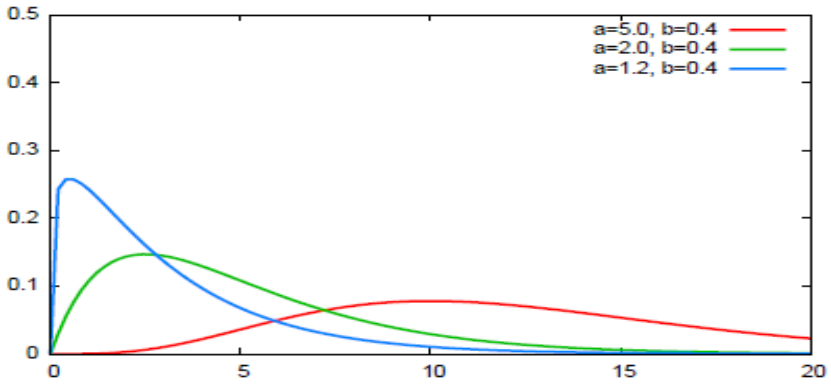
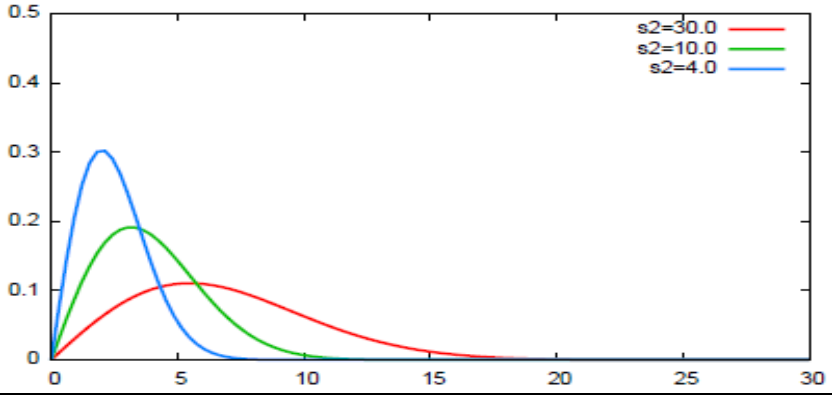
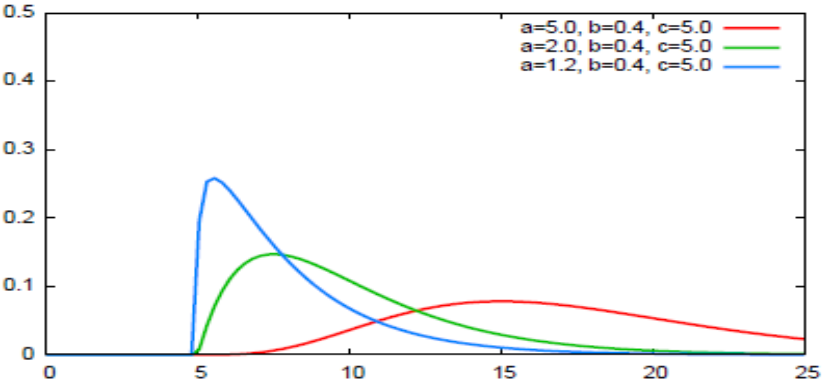
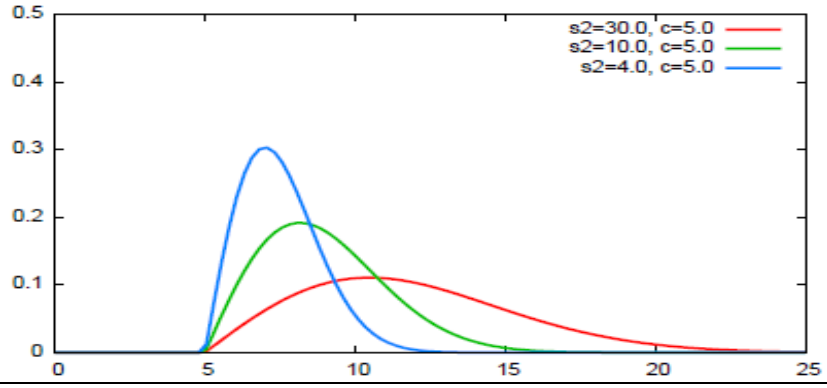
Таблица 5 – Распределения вероятностей, используемые для моделирования поведения односторонней задержки

Распределение	Функция плотности	Область значений	Мат. ожидание	Дисперсия
Гамма-распределение	$G(x\|\alpha,\beta) = x^{\alpha-1}\cdot\frac{\beta^{\alpha}\cdot e^{-\beta x}}{\Gamma(\alpha)}$	$[0,\infty)$	$\frac{\alpha}{\beta}$	$\frac{\alpha}{\beta^2}$
Распределение Рэлея	$R(x\|\sigma^2) = \frac{x\cdot\exp(-\frac{x^2}{2\sigma^2})}{\sigma^2}$	$[0,\infty)$	$\sigma\sqrt{\frac{\pi}{2}}$	$\frac{4-\pi}{2}\sigma^2$
Смещенное гамма-распределение	$\check{G}(x\|\alpha,\beta,c) = \begin{cases} G(x-c\|\alpha,\beta), x > c \\ 0, x \le c \end{cases}$	$[0,\infty)$	$\frac{\alpha}{\beta}+c$	$\frac{\alpha}{\beta^2}$
Смещенное распределение Рэлея	$\check{R}(x\|\sigma^2,c) = \begin{cases} R(x-c\|\sigma^2), x > c \\ 0, x \le c \end{cases}$	$[0,\infty)$	$\sigma\sqrt{\frac{\pi}{2}}+c$	$\frac{4-\pi}{2}\sigma^2$

Таким образом, проведенный выше качественный обзор научно-методического аппарата анализа временных рядов показал, что каждый из рассмотренных методов имеет свои достоинства и недостатки. В силу наличия временных рядов с регулярными периодическими компонентами в различных сферах науки, решение задачи их прогнозирования является важной и актуальной научно-технической задачей, что подтверждает необходимость формирования самостоятельной методики прогнозирования (превентивной идентификации) аномальной ситуации во временном ряду метрик сетевых элементов распределенной ИТКС, позволяющей в явном виде учесть эти компоненты и отвечающей следующим свойствам:

– инвариантности относительно обрабатываемых метрик разнородных сетевых элементов ИТКС в рамках выбранного класса прогнозируемых процессов;
– учета взаимосвязи сечений не только на интервале периодичности случайного процесса, но также для тренда и его случайной компоненты (центрированного случайного процесса);
– возможности регуляризации временного ряда по небольшому числу параметров;
– наличия теоретически обоснованного алгоритма оптимизации.

Таблица 6 – Графики функций плотности распределения вероятностей для моделирования поведения односторонней задержки

Распределение	Функция плотности распределения вероятностей
Гамма-распределение	
Распределение Рэлея	
Смещенное гамма-распределение	
Смещенное распределение Рэлея	

7. Символьное представление временных рядов

Рассматривая поведенческий подход к мониторингу ИТКС, необходимо отметить, что независимо от отечественной или международной классификации состояний технических устройств [7, 12], в итоге, интерпретация таких ТС сводится к двум основным: «норма» – сетевой элемент выполняет свои функции и «авария» – сетевой элемент не может выполнять свои функции. Остальные состояния служат лишь для уведомления оператора о смене ТС и о направлении динамики процесса – от «нормы» к «аварии», от «аварии» к «норме».

Динамика переходных процессов от «нормы» (*N*) к «аварии» (*F*) [12] редко характеризуется явной последовательностью событий *N* – *I* – *J* – *C* – *F*. Как правило, в журнале регистрации событий наблюдается переходные процессы с колебаниями, при которых вполне возможен как временный возврат на менее критическое состояние, так и резкие скачки «через» состояние или несколько состояний (например: *N* – *I* – *J* – *C* – *F*; *N* – *J* – *C* – *F*; *N* – *C* – *F*; или даже *N* – *F*), которые не были идентифицированы по причине малой скважности опроса сетевого элемента сервером мониторинга.

Решение вопроса периодичности опроса объектов мониторинга подсистемой контроля является самостоятельной оптимизационной задачей, но, в то же время, полученное ее решение не будет универсальным на множестве контролируемых метрик для разнородных сетевых элементов различных ИТКС. Каждый производитель старается решить данную задачу для своего оборудования самостоятельно. Так, для временных рядов, характеризующихся трендом случайного процесса (рис. 12 *а*), наиболее используемым в подсистемах мониторинга является триггерный механизм идентификации технического состояния (например, активно используемый в Cisco), позволяющий устранить дублирование событий в журнале в случае колебаний измеримой характеристики вблизи порога (т. н. эффект «дребезга нуля», рис. 1), но даже он не приводит к надежной идентификации направления динамики процесса.

Поэтому нужен поиск новых подходов к решению такого класса задач.

Рассмотрим временной ряд с использованием символьного представления, описанного в [60] и применяемого в разделе символической динамики, когда для описания последовательностей измерений состояния системы пользуются символами некоторого заданного алфавита. Такой подход наиболее эффективен в описании и исследовании детерминированных систем, в которых из-за ограничений возможностей измерения возникает сходство со случайным процессом. При этом описание временного ряда и динамики его изменения возможно в терминах топологических аналогов марковских процессов, т. е. с помощью матриц возможных переходов между классами ТС системы. Непосредственно для такого описания необходимо задать алфавит, который бы наиболее подходил для представления разбиения пространства ее состояний на области, которые бы соответствовали измеряемым значениям параметров.

Данная оценка была заимствована теорией символической динамики из биоинформатики, где активно используется для оценки сложности нуклеотидных геномных последовательностей [63], например, очень длинных последовательностей ДНК [64], рис. 18.

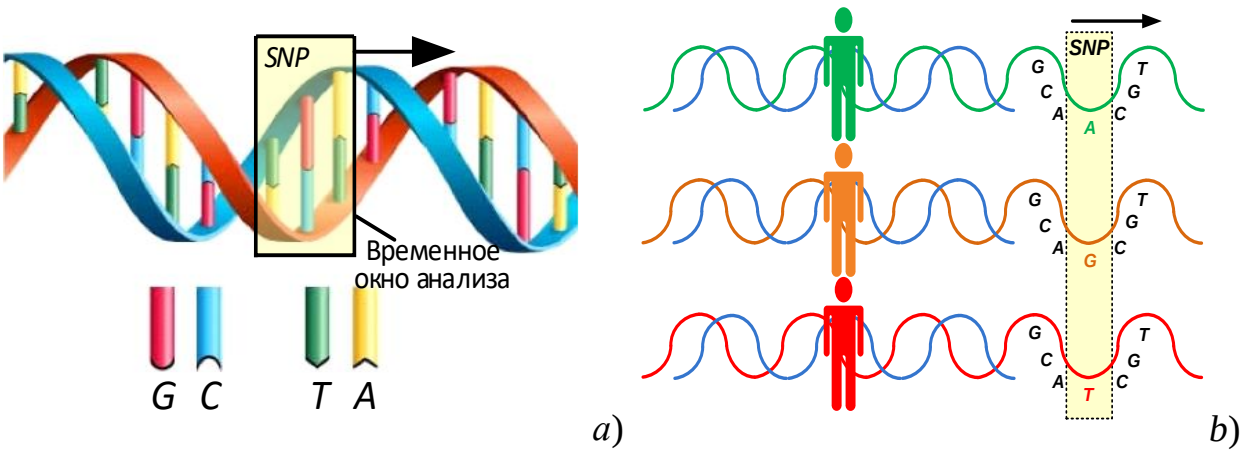


Рис. 18. Процесс анализа сложных нуклеотидных геномных последовательностей методом символической динамики

Вполне естественно оценивать сложную бесконечную допустимую последовательность числом различных конечных слов (например, с элементами алфавита $\{G, C, T, A\}$), входящих в нее. Тогда задача определения вторичной структуры временного ряда (структуры локальных конфигураций) формулируется как задача преобразования слов в алфавите метрик в слова над алфавитом локальных конфигураций, используя метод скользящего окна (кодов определенных слогов в кодовых словах). При этом количественная оценка временного ряда может быть произведена с помощью топологической энтропии или метрической энтропии по Колмогорову [65].

Постановка задачи. Рассмотрим временной ряд произвольной природы $T = \{(f_i, t_i), \ i = \overline{1,n}\}$, где f_i – значение характеристики наблюдаемого процесса в момент времени t_i, n – число наблюдений (временных отсчетов).

Необходимо определить обобщенные универсальные характеристики данного временного ряда, по которым возможно оценить разнообразие наблюдаемых значений параметров (метрик), относящихся к определенной области состояния объекта мониторинга (классу его технического состояния).

Для решения задачи на первом этапе осуществляем символьное кодирование временного ряда по возможным значениям параметров (метрик).

7.1. Анализ временного ряда по значениям метрик

Необходимость универсализации разнородных временных рядов в пространстве их кластеризации налагает требования к их обобщенным универсальным характеристикам, определенные значения которых интерпретируются координатами точки, которая представляет рассматриваемый временной ряд в таком пространстве. В то же время сложности универсализации связаны с тем, что различные временные ряды имеют разную точность измерений, т. е. число значащих цифр в значении характеристики наблюдаемого процесса f_i, а также вариацию этих значений на разных интервалах времени t_i, что видно из рис. 19.

Для универсализации временных рядов в [62] предлагается масштабирование значений наблюдаемой функции f_i, а также построение исходя из этого строки символов, которые отражали бы динамику их числовых значений. Для

этого определяется размах варьирования значений рассматриваемого временного ряда: $V = y_{max} - y_{min}$, где $y_{min} = \min\limits_{i=\overline{1,n}} f_i$, $y_{max} = \max\limits_{i=\overline{1,n}} f_i$, на котором вводится разбиение y_i, $i = \overline{1,m}$ диапазона $[y_1, y_m]$, причем $y_1 = y_{min}$, $y_m = y_{max}$. Однако, поскольку значения f_i временного ряда могут попадать и на границу разбиений, то в данном случае правильнее рассматривать диапазон $[y_i, y_{i+1}) = \{y \mid y_i \le y < y_{i+1}, i = \overline{1,m-1}\}$. Тогда определение числа разбиений k ($k = m - 1$) всего диапазона наблюдения значений параметра (метрики) на сегменты, а также определение их внутренних границ является самостоятельной оптимизационной задачей [52] с применением бикритериального метода построения гистограмм, которая уже была решена в [66]. Число разбиений k диапазона наблюдения параметра, полученных данным методом и определяет мощность алфавита описания.

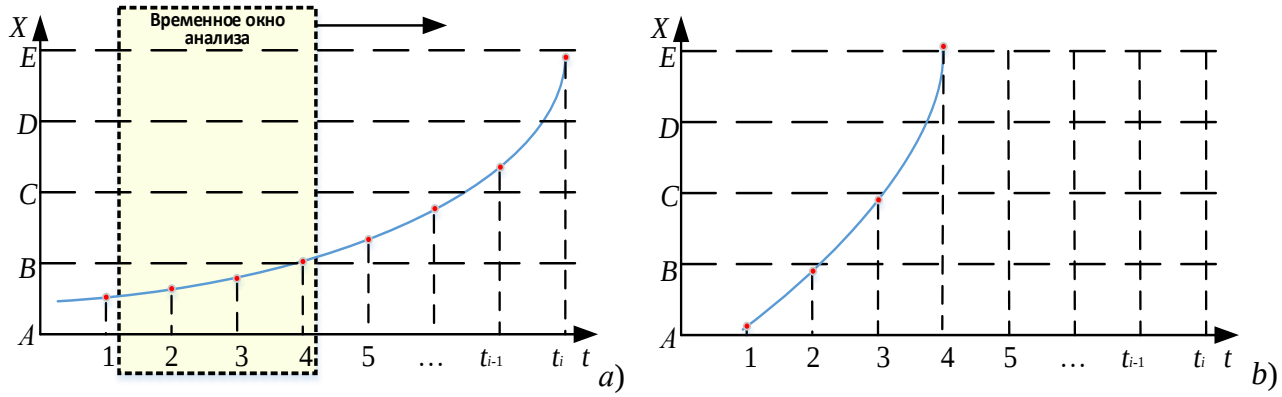


Рис. 19. Символьное представление временного ряда наблюдаемого параметра *a*) с медленным и *b*) лавинообразным нарастанием аварийной ситуации (отказа)

Например, на рис. 19 приведено разбиение размаха временного ряда на символы *A*, *B*, *C*, *D*, *E* выбранного алфавита Σ (здесь символы алфавита Σ соответствуют прописным символам латинского алфавита). При этом последний элемент разбиения (на рис. 19 обозначен как «*E*»), очевидно также будет являться сегментом. Данными символами обозначаются разбиения значений наблюдаемой величины в порядке их возрастания. Так символ «*A*» – имя разбиения наименьших значений (по видам состояния [7] соответствует исправному техническому состоянию сетевого элемента, когда все параметры имеют номинальные значения), а «*E*» – наибольших значений, соответствующее аварии (отказу).

Если измерения параметра (метрики) ведется в дискретное время, то описание значений временного ряда символами разбиений есть слово над алфавитом Σ в строке. Прохождением по временному ряду получается кодирование (представление) его строкой символов. Причем числовое значение f_i кодируется символом разбиения (сегмента), в котором оно находится: для рис. 19 *a*) – {*AAABBBCD*…}; для рис. 19 *b*) – {*AABE*…}. Если наблюдаемый процесс описывается резким увеличением значений параметра (наблюдаемой величины), равно как и резким спадом за один временной интервал относительно нормаль-

ного тренда его изменения (последовательного перехода из одного разбиения (сегмента) в другой), то получаемые кодовые слова, характеризующие временной ряд не будут содержать некоторых слогов. Так, кодовое слово временного ряда показанного на рис. 19 *b*) не содержит слога «*CD*». Данная ситуация идентифицируется как лавинообразный процесс развития аварии (отказа).

Такой подход позволяет осуществить интервальный анализ временного ряда, где в качестве интервала может рассматриваться «скользящее окно», последовательно сдвигающееся вдоль временного ряда и отслеживающее появление аномальных предаварийных ситуаций, или отказов, путем сравнения просматриваемых в «скользящем окне» слогов в наблюдаемом кодовом словестроке временного ряда с «запрещенными» кодовыми слогами, идентифицирующими аномальное состояние.

При этом временной ряд, имеющий n временных отсчетов (наблюдений), будет представлен в виде кодового слова-строки из n символов над алфавитом Σ, а ширину «скользящего окна» можно подобрать оптимальным образом (для конкретной метрики индивидуально), учитывая физические процессы развития аномальных ситуаций и отказов в различных сетевых элементах, при различных режимах и условиях функционирования. Так, на рис. 19 *a*) ширина скользящего окна анализа равна $m = 3$. Поскольку процессу возникновения отказа сетевого элемента, как правило, предшествуют во времени изменения значений параметров (метрик) с трендом выхода их за пределы эксплуатационных и профилактических допусков [67], то в ходе производственных испытаний и опытной эксплуатации технических устройств нарабатывается база «запрещенных» слогов кодовых слов, используемая в пространстве сдвигов «скользящего окна» путем сравнения с наблюдаемым результатом.

Таким образом, выявление «запрещенных» слогов в кодовом словестроке временного ряда может лечь в основу метода прогнозирования наступления аварии или отказа.

Для решения задачи масштабирования в [63] предложен диапазон значений временного ряда, который может быть как с равномерным разбиением, так и с вычислением длины и числа разбиений на основе аппарата математической статистики (при решении задач мониторинга – аппарата теории надежности). Для временных рядов конкретных контролируемых параметров данный вопрос индивидуален и зависит не только от номинальных величин параметра, но также от эксплуатационных и профилактических допусков на них [67]. Число разбиений при оценке функциональной надежности сетевых элементов, как правило, соответствует видам их ТС [7, 12].

Как отмечалось ранее, в соответствие с [7] различают следующие виды технического состояния: исправное, неисправное, работоспособное, неработоспособное, предельное, опасное и предотказное состояние. В то же время, с точки зрения функциональной надежности нас в большей степени интересует переход из работоспособного в неработоспособное («Авария» или «Отказ») состояние через промежуточное – предотказное техническое состояние. Учитывая это, разбиение, соответствующее предотказному техническому состоянию может уточняться для каждого сетевого элемента или его измеряемого параметра.

№4. 2021
ISSN 2410-9916

Очевидно, что различные временные ряды могут содержать не равные количества наблюдаемых значений. В рассматриваемом подходе символьного кодирования это означает, что описание временного ряда будет представлено словами-строками различной длины в заданном фиксированном алфавите. В связи с чем, в [65] осуществлен переход от оценки абсолютной сложности строки по Колмогорову (от длины сжатой строки) к ее относительной оценке через коэффициент сжатия [49, 50].

7.2. Анализ временного ряда по тенденциям

В ряде случаев для подсистемы мониторинга функциональной безопасности (надежности) интерес представляет не реальное изменение временного ряда в следующий дискрет времени, а изменение его тенденции. Сама по себе задача определения рациональных порогов идентификации в изменении тенденций достаточно сложна, поскольку необходимо определиться с критерием положительной тенденции или ее отсутствием (0,5 %, 1 %, 2 %...?). При этом необходима либо специальная предварительная обработка исходных данных временных рядов, либо применение метода экспертных оценок, что, во втором случае носит субъективный характер и не является математически обоснованным.

Само по себе использование метода символьного кодирования значений временного ряда уже можно интерпретировать как предварительную обработку, а поскольку используемый в [65] бикритериальный метод построения разбиений гарантирует, что доверительный интервал для выборочного среднего в каждом разбиении будет не шире самого разбиения, то локализация значений, кодируемых одним символом алфавита Σ, является статистически достоверной.

Из чего можно заключить, что, используя метод символьного кодирования, изменение символа заданного для временного ряда алфавита Σ в следующий временной интервал и есть квалификация тенденции, в то время как изменение значения параметра, не выводящее его за полосу ширины разбиения – отсутствие какой-либо тенденции.

Продемонстрируем символьное описание временного ряда изменения значений параметра по тенденциям на примере рис. 20.

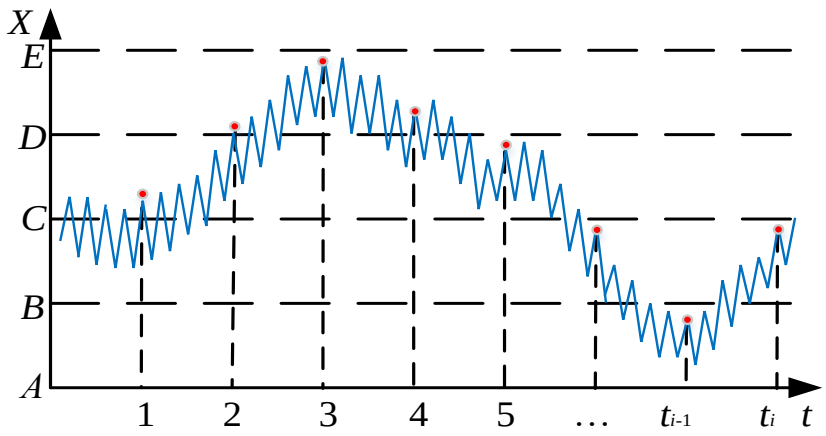


Рис. 20. Символьное описание временного ряда изменения значения параметра

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

Для кодирования *по тенденциям* представленного на данном рисунке временного ряда используем алфавит $\Sigma_т$ = {–, 0, +}, в котором символом «0» обозначено отсутствие тенденции в значении последующего временного интервала. Тогда при кодировании временного ряда в ранее определенном алфавите $\Sigma_{знач}$ = {*A*, *B*, *C*, *D*, *E*} (*по значениям*) кодовое слово будет иметь вид: {*CDDDCBAB*}, а при кодировании того же временного ряда по тенденциям с использованием алфавита $\Sigma_{тенд}$ кодовое слово будет выглядеть как{0+00–––+}, предполагая, что первый символ кода тенденции всегда имеет значение «0» (отсутствие тенденции).

С точки зрения теории надежности для подсистемы мониторинга важно, чтобы значения наблюдаемых параметров сетевых элементов находились при определенных режимах функционирования в стабильном состоянии (отсутствие тенденций). Для динамических систем с постоянно изменяющимися режимами работы (недогруженный, перегруженный и пр.) и изменением обрабатываемой нагрузки в символах кодовых слов, описывающие временные ряды наблюдаемых параметров всегда будут присутствовать тенденции.

Для выявления разрушительных тенденций, вызывающих переход сетевого элемента из работоспособного состояния в состояние отказа (аварийное состояние) необходимо определить запрещенные полуслова (слоги) в описываемом временной ряд слове-строке. Как правило, аварийному режиму функционирования предшествует некоторый временной интервал, соответствующий предотказному состоянию, характеризуемый повышенным риском возникновения отказа (аварии) [7, 68].

Предотказное состояние может быть связано с воздействиями на сетевой элемент многих внешних (ошибки персонала, условия эксплуатации, воздействия естественного и искусственного характера и пр.) и внутренних (производственные дефекты, программные сбои, перегруженные режимы работы и пр.) факторов. При этом задачей подсистемы мониторинга является своевременное обнаружение предотказного состояния сетевого устройства с целью оперативного (превентивного) принятия мер для недопущения развития отказа.

С этих позиций применение метода символьного кодирования как по значениям временных рядов, так и по тенденциям, позволяет заблаговременно обнаружить «запрещенную» комбинацию полуслов (слогов) в кодовом слове, описывающем временной ряд значений контролируемых параметров. Тогда обнаружение развития отказа возможно по выявлению в кодовом слове временного ряда слогов, идентифицирующих стремительно развивающуюся тенденцию в сторону разбиения, характеризующего аварийной состояние объекта контроля (для рассматриваемого примера рис. 19 и 20 – разбиение «*E*»).

Так, при символьном кодировании значений временного ряда на рис. 19 *a*) факт перехода из режима нормального функционирования (символ разбиения – «*A*») к предотказному ТС (символ разбиения «*D*») интерпретируют слогом «*BCD*» в слове-строке {*AAABBBCD*…}, а на рис. 19 *b*) переход к отказу – слогом «*ABE*» в слове {*AABE*}. При кодировании временного ряда по тенденциям аномальное состояние (поведение) системы (сетевого устройства) может идентифицироваться слогами типа {+ +}, {+ + +}, или {– –}, {– – –}.

Соответственно подсистема мониторинга должна в ходе обработки кодового слова временного ряда выявлять подобные «запрещенные» комбинации слогов, характеризующие наступление предотказного состояния или отказа системы. Факт перехода объекта мониторинга в критическое состояние должен выявляться заранее для принятия превентивного управляющего воздействия. Такой реакцией подсистемы мониторинга на наступление предотказного ТС может быть управляющее воздействие на сеть (сетевой элемент) или перевода системы мониторинга в *особый режим мониторинга*.

В работе предлагается в качестве особого режима мониторинга использовать увеличение скважности опросов сервером мониторинга сетевого элемента по значениям наблюдаемых метрик, когда при выявлении наступления его предотказного состояния по агрегированной предварительно собранной статистике о сетевом устройстве для недопущения развития аварийной ситуации частота опроса объекта мониторинга увеличивается, например, в 10 раз, т. е. вместо 1 раза в 5 минут, опрос осуществляют каждые 30 секунд или еще чаще.

8. Научно-методический аппарат анализа временных рядов

Предметом настоящего исследования является научно-методический аппарат выявления нестационарных состояний ОК, на котором проводится измерение. В такой постановке сформулируем и решим следующие задачи анализа временных рядов, закодированных методами теории символической динамики:

– символьное кодирования значений временного ряда и способ кодирования его участков (ячеек) вектором *оценок энтропии сдвигов*;
– *обучение классификатора* состояний объекта измерения на основе энтропии сдвигов;
– *классификация состояния* по тестовой выборке измерений, в которых измеряемая характеристика описывается своим распределением вероятностей сдвигов.

8.1. Оценка энтропии кодового слова, описывающего временной ряд наблюдаемой метрики

Для выявления в кодовом слове-строке анализируемого временного ряда «запрещенных» слогов, идентифицирующих развитие аварии воспользуемся оценкой энтропии слов [52]. При этом оценку энтропии кодовых слов описывающего временной ряд наблюдаемого параметра осуществляют в следующем порядке [52]. Сначала фиксируют длину слога m и алфавит Σ. Множество различных слогов на выбранном алфавите составит Σ^m. Соответственно мощность этого множества $M = |\Sigma^m|$ составляет общее число слогов. Если обозначить k – мощность алфавита, то $M = k^m$. Для фиксированной длины слогов m вводится произвольная их нумерация $i = \overline{1, M}$, а также счетчики числа слогов c_i. В ходе анализа временного ряда T длиной n, происходит сдвиг временного окна шириной m на один интервал $[t_i, t_{i+1}]$. Таким образом, имеется $n - m + 1$ позиций временного окна, для каждой из которых идентифицируется слог, полученный в окне. Если в текущей позиции окна шириной m наблюдается слог, имеющий в принятой нумерации номер $i = \overline{1, M}$, то значение счетчика числа слогов c_i воз-

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

растает на единицу. Тогда по полученным значениям счетчика c_i осуществляется оценка энтропии слов по выражению

$$C_m = -\sum_{i=1}^{M}\left(\frac{c_i}{n-m+1}\right)\log_m\left(\frac{c_i}{n-m+1}\right). \quad (1)$$

Использование в качестве основания алгоритма мощности различных слогов M автоматически нормирует значение энтропии слов C_m. Ситуация, когда $C(m) = 0$ означает, что все слоги длиной m одинаковы и состоят из одного и того же слога или при длине слога совпадающим с длиной наблюдаемого кодового слова, т. е. $m = n$, мы имеем только один слог. А случай, когда $C(m) = 1$, соответствует одинаковой частоте встречаемости всех возможных слогов из Σ^m в наблюдаемом кодовом слове-строке (частота символов алфавита одинакова в исходном кодовом слове). В результате оценки энтропии слов можно построить функцию $C(m) = C_m$, с аргументом m ($1 \leq m \leq n$), которая вычисляется при фиксированном m по анализируемому временному ряду в соответствие в выражением (1) и увеличением на единицу ширины окна на области определения m от 1 до n.

В соответствии с терминами символической динамики [69], функцию $C(m)$ называют оценкой энтропии сдвигов.

Проведем для каждой ячейки (участка временного ряда) процедуру вычисления энтропии сдвигов последовательно с возрастающей шириной окна $m = \overline{1,W}$. В результате получим вектор энтропийной характеристики ячейки u_i:

$$\boldsymbol{h} = (C_1, C_2, \ldots, C_m). \quad (2)$$

8.2. Метод обучения классификатора состояний объекта мониторинга на основе энтропии сдвигов

В основе предложенного метода лежит предположение, что любая ячейка исходного временного ряда принадлежит ко всем формируемым состояниям C_k, $k = \overline{1,M}$, но с разной вероятностью. Тогда задача будет заключаться в «подгонке» распределений «смеси состояний» к данным ячеек, а затем в определении вероятностей принадлежности измеренного вектора наблюдения к каждому состоянию.

Построим гистограмму энтропии для каждой компоненты введенного ранее вектора h. По оси x изменяется величина энтропии от 0 до 1, а по оси y – количество ячеек с данной величиной энтропии. Количество интервалов энтропии положим равным E.

Будем считать, что каждая гистограмма (для каждой компоненты $\boldsymbol{h} = (C_1, C_2, \ldots, C_m)$) представляет собой смесь функций Гаусса

$$p(h|\theta) = \sum_{m=1}^{K}\pi_m \cdot N(h|\mu_m, \sigma_m^2), \quad (3)$$

где π коэффициенты участия компонентов функций Гаусса в смеси, удовлетворяющие свойству $\sum\pi_k=1$. Таким образом, $p(h)$ представляет собой плотность распределения вероятностей энтропии сдвигов. Для указанной плотности рассмотрим логарифмическую функцию правдоподобия:

$$L(\theta) = \ln\left(\prod_i p(h_i|\theta)\right) = \ln\left(\prod_i \sum_{k=1}^{K} \pi_k \cdot N(h_i|\mu_k, \sigma_k^2)\right) =$$
$$= \sum_i \ln\left(\sum_{k=1}^{K} \pi_k \cdot N(h_i|\mu_k, \sigma_k^2)\right), \quad (4)$$

где $\theta \in \{\pi_k, \mu_k, \sigma^2{}_k\}$, $k \in \{1, ..., K\}$.

Для максимизации функции продифференцируем ее по параметру μ_k.

Для краткости положим $\phi_k(h_i) = N(h_i \mid \mu_k, \sigma^2{}_k)$,

$$\frac{\partial L(\theta)}{\partial \mu_k} = \sum_i \frac{1}{\sum_{k=1}^{K} \pi_k \varphi_k(h_i)} \pi_k \frac{\partial \phi_k(h_i)}{\partial \mu_k} = \sum_i \frac{\pi_k \cdot \phi_k(h_i)}{\sum_{k=1}^{K} \pi_k \cdot \phi_k(h_i)} \frac{1}{\phi_k(h_i)} \frac{\partial \phi_k(h_i)}{\partial \mu_k} =$$
$$= \sum_i \frac{\pi_k \cdot \phi_k(h_i)}{\sum_{k=1}^{K} \pi_k \varphi_k(h_i)} \frac{\partial \ln(\phi_k(h_i))}{\partial \mu_k}. \quad (5)$$

Значение $\partial \ln \phi_k(x_i)/\partial \mu_k$ представляет собой производную логарифмической функции правдоподобия функции Гаусса и может быть использовано для установления параметров несмешанной модели. Наибольшие сложности при нахождении максимума вызывают сомножители $\frac{\pi_k \phi_k(x_i)}{\sum_k \pi_k \phi_k(x_i)}$ также зависящие от переменных.

Введем скрытую переменную $z \in \{1, ..., K\}$, указывающую, что данная точка h пришла из k-го гауссиана. Тогда определим,

$$p(z = k) = \pi_k, \quad (6)$$

$$p(h|z = k) = \pi_k N(h_i|\mu_k, \sigma_k^2), \quad (7)$$

$$p(h) = \sum_{k=1}^{K} p(h|z = k) = \sum_{k=1}^{K} \pi_k N(h_i|\mu_k, \sigma_k^2). \quad (8)$$

Это разлагает гауссову смесь на скрытую переменную z и параметры модели θ, которые позволяют выяснить, из какого гауссова значения была получена каждая точка данных. При этом вероятность получения точки из k-го гауссиана равна

$$p(z = k|h, \theta) = \frac{p(h, z = k; \theta)}{\sum_k p(h, z = k; \theta)}. \quad (9)$$

Указанная величина может выступать весовым коэффициентом в рассмотренной производной функции правдоподобия. Если мы знаем z, т. е. из какого гауссовского значения получены данные, нам больше не нужно суммировать по всем K гауссианам ($\Sigma\, p(x, z)$), чтобы максимизировать предельную вероятность. Вместо этого рассматриваем на каждом подмножестве x, исходящем из k-го гауссиана, и можем оценить θ_k как

$$\arg\max_{\theta_k} \sum_i \ln p(h_i; \theta_k) \forall i(z_i = k). \quad (10)$$

Если мы знаем, по какой гауссовой компоненте была получена точка данных (скрытая переменная z), то мы можем максимизировать логарифмическую вероятность и получить оценки параметров модели. В свою очередь, если известны параметры модели, можно вычислить апостериорную вероятность z, которая позволит оценить, из какого гауссова значения пришла каждая точка данных. Вместо того, чтобы одновременно вычислять оптимальную скрытую переменную z и параметр модели θ, мы по очереди будем оптимизировать каждую из них, до нахождения точной оценки. Указанные соображения позволяют использовать для разделения смеси распределений энтропии сдвигов *EM*-алгоритм [70], состоящий из следующих двух шагов:

1. *E-шаг*. На каждом *E*-шаге вычислим текущие вероятности принадлежности точек h k-й компоненте распределения вероятностей энтропии по формуле:

$$z_{ik} = \frac{\pi_k N\left(h_i \middle| \mu_k, \sigma_k^2\right)}{\sum \pi_m N\left(h_i \middle| \mu_k, \sigma_k^2\right)}. \tag{11}$$

2. *M-шаг*. На каждом *M* шаге вычисляются новые оценки параметров μ_k, σ^2_k путем максимизации нижней оценки $Q(\theta)$ приведенной выше логарифмической функции правдоподобия $L(\theta)$, полученной из условия выпуклости $L(\theta)$ путем применения неравенства Йенсена с подстановкой соответствующих параметров, вычисленных на предыдущем шаге.

$$Q\left(\theta;\theta^t\right) = \sum_i \sum_k z_{ik} \ln\left(\pi_k \cdot N\left(h_i \middle| \mu_k, \sigma_k^2\right)\right). \tag{12}$$

Найдя частные производные указанного выражения:

$$\begin{aligned} &\frac{\partial Q\left(\theta;\theta^t\right)}{\partial \mu_k} = 0, \\ &\frac{\partial Q\left(\theta;\theta^t\right)}{\partial \sigma_k^2} = 0, \\ &\frac{\partial Q\left(\theta;\theta^t\right)}{\partial \pi_k} = 0, \end{aligned} \tag{13}$$

получим выражения для обновления текущих значений:

$$\mu_k^{(e+1)} = \frac{\sum_{i=1}^{n} z_{ik}^{(t)} h_i}{\sum_{i=1}^{n} z_{ik}^{(t)}}, \tag{14}$$

$$\sigma_k^{2(t+1)} = \frac{\sum_{i=1}^{n} z_{ik}^{(t)} \left(h_i - \mu_k^{(t+1)}\right)^2}{\sum_{i=1}^{n} z_{ik}^{(t)}}. \tag{15}$$

Результирующее правило обновления для π_k идентично для любого типа смешанных моделей и может быть определенно как:

$$\pi_k = \frac{1}{n}\sum_{i=1}^{n} z_{ik} = \frac{N_k}{n}, \quad (16)$$

где N_k – ненормализованный вес компонента k: $N_k = \sum_{i=1}^{n} z_{ik}$.

$$\pi_k^{(t+1)} = \frac{\sum_{i=1}^{n} z_{ik}^{(t)}}{n}. \quad (17)$$

8.3. Классификация состояния сетевого устройства

После определения параметров распределения вероятностей для каждого из состояний C_k, $k = \overline{1, M}$ для оперативной оценки текущего состояния объекта измерений можно использовать теорему Байеса.

Допустим, в процессе измерения была получена выборка $X = (x_1, x_2, ..., x_n)$. К указанной выборке производится добавление «хвоста», – l измерений, полученных на предыдущих шагах. К полученной в результате выборке $X = (x_1, x_2, ..., x_l, \ldots, x_{l+n})$ применяется процедура разбивки на ограниченное число ячеек u_i с вычислением в каждой из них вектора энтропии сдвигов $h(u_i)$, рассмотренного выше.

В результате полученный набор векторов энтропии сдвигов по каждой их проекции (обозначим ее как случайную величину H) проверяется на принадлежность к каждому из состояний на основании апостериорных вероятностей $P(C=k|h)$.

Формально правило классификации может быть выражено как:

$$H \sim C_k \Leftrightarrow k = \arg\max_i P\left(C = i \middle| H\right). \quad (18)$$

Иными словами, X принадлежит к классу C_k, если апостериорная вероятность $P(C=k|H)$ максимальна.

Предполагая, что n измерений выборки X независимы и распределены одинаково получаем вероятности принадлежности выборки $H = (h_1, ..., h_n)$ состояниям C_k:

$$P\left(H \middle| C = k\right) = \prod_{i=1}^{n} N\left(h_i \middle| \mu_k, \sigma_k^2\right). \quad (19)$$

Априорные вероятности $P(\mathrm{C} = k)$ для M состояний C_k, $k = \overline{1, M}$, будем полагать одинаковыми:

$$P\left(C = k\right) = \frac{1}{M}. \quad (20)$$

Вероятность $P(C = k|H)$ того, что, полученная проекция энтропии H была произведена k-й компонентой можно определить через теорему Байеса:

$$P\left(C = k \middle| H\right) = \frac{P\left(H \middle| C = k\right)P\left(C = k\right)}{P\left(H\right)} = \frac{P\left(H \middle| C = k\right)P\left(C = k\right)}{\sum P\left(H \middle| C = i\right)P\left(C = i\right)}. \quad (21)$$

Полученный в результате набор вероятностей принадлежности состояниям при помощи логических правил принятия решений используется для генерации событий оператору системы мониторинга.

Для исследования качества процесса классификации состояния сетевого устройства по предложенному алгоритму на основе статистики энтропии сдвигов был поставлен эксперимент на основе упомянутого набора данных недельной загрузки процессора сервера виртуализации.

Результаты эксперимента показаны в таблице 7. Здесь для фиксированного интервала (50) точек наблюдения временного ряда (синий цвет на левых рисунках таблицы 7) и окон вычисления энтропии размером 2, 3, 5 и 7 была вычислена статистика энтропии сдвигов (красный и зеленый цвет на левых рисунках таблицы 7), в виде гистограмм (правые рисунки таблицы 7), которые аппроксимированы тремя нормальными распределениями вышеописанным *EM*-алгоритмом, со следующими значениями метрик математического ожидания *m* и дисперсии *D*:

– для ширины скользящего окна – 2: m = 0; 1,23; 2,29, D = 0,13; 0,09; 0;
– для ширины скользящего окна – 3; m = 0; 1,58; 2,48, $D = 10^{-6}$; 0,15; 0,12;
– для ширины скользящего окна – 5: m = 0,02; 1,7; 2,41, D = 0.07; 0,003; 0,12;
– для ширины скользящего окна – 7: m = 0,01; 2,13; 2,63, $D = 10^{-5}$; 0,01; 0,1.

Таким образом, как видно из таблицы 7, наиболее четкое разделение состояний (без нагрузки, переходное состояние, перегрузка) наблюдается для энтропийных окон шириной 2 и 3.

С возрастанием размера скользящего окна качество аппроксимации визуально ухудшается, что затрудняет процесс классификации состояния сетевого устройства.

Описанный подход с классификацией состояния элементов телекоммуникационной сети неплохо работает в случае возможности выделения классов поведений. Это было продемонстрировано для односторонней задержки [60], когда компонента, связанная с маршрутизацией (ожидание в очередях), включается в общее выражение задержки лишь при средних и высоких нагрузках. В меньшей степени этот метод может быть использован для оценки состояния загрузки вычислительных ресурсов, в частности процессора. Хотя и здесь имеет место задержка, связанная с переключением контекста вычисления, но она более связана с организацией вычислительного процесса, чем с режимом нагрузки. В этом случае требуется предварительный этап уточнения числа состояний и соответствующих им распределений. Это продемонстрировано на рисунках таблицы 7, где приведена попытка аппроксимации гистограммы статистики недельной загрузки процессора сервера виртуализации двумя и тремя нормальными распределениями по смешанной гауссовской модели *EM*-алгоритмом.

Последовательность действий на этапе обучения классификатора с использованием процедуры *EM*-алгоритма, а также при выполнении этапа классификации состояния сетевого элемента представлено на рис. 21. Данные этапы в последующем будут включены в общую методику превентивной идентификации аномального состояния сетевого элемента на временных рядах его метрик.

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

Таблица 7 – Модельный пример

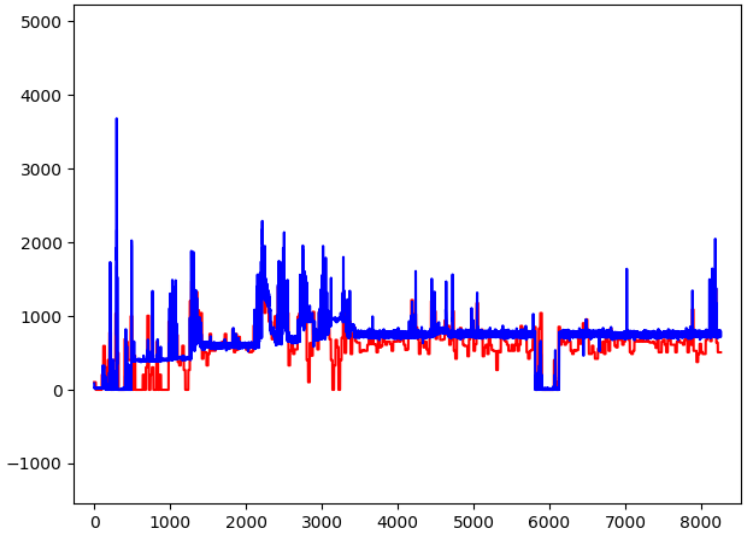
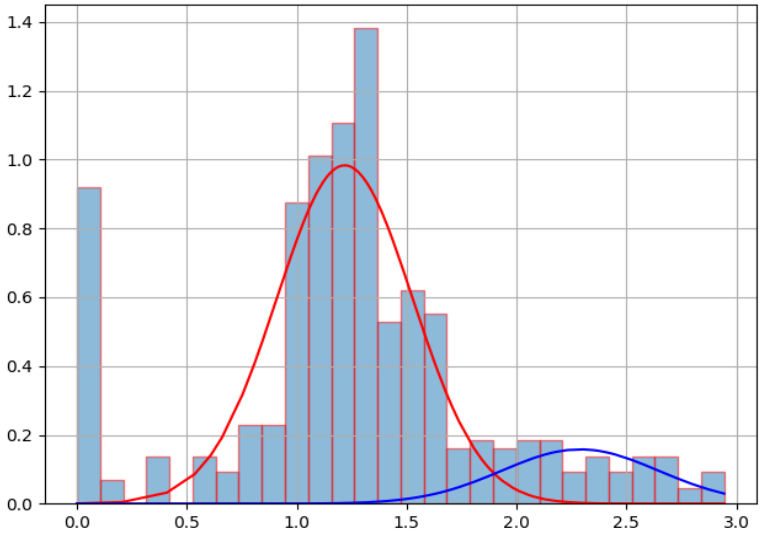
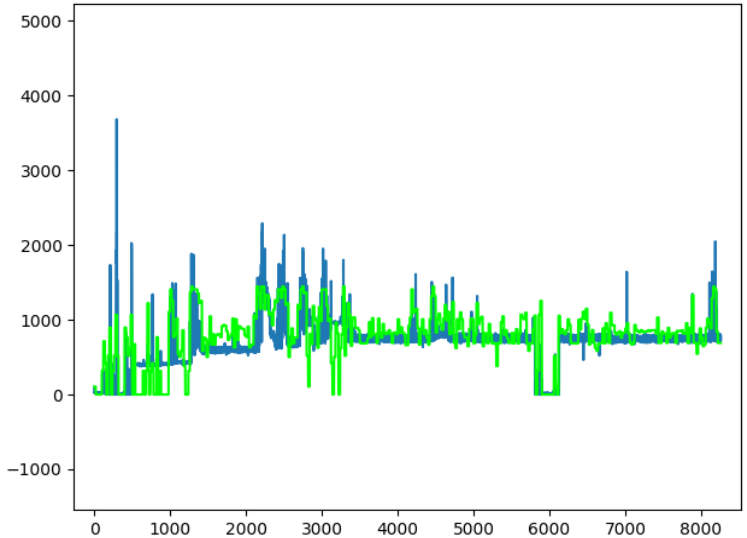
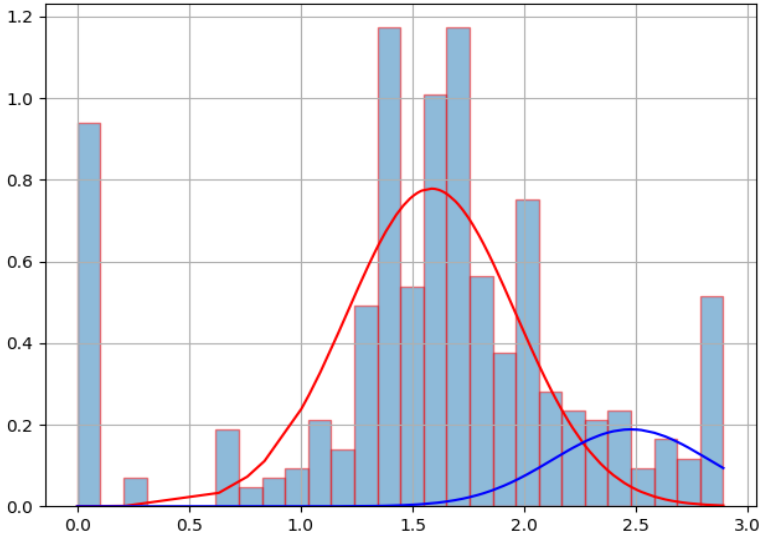
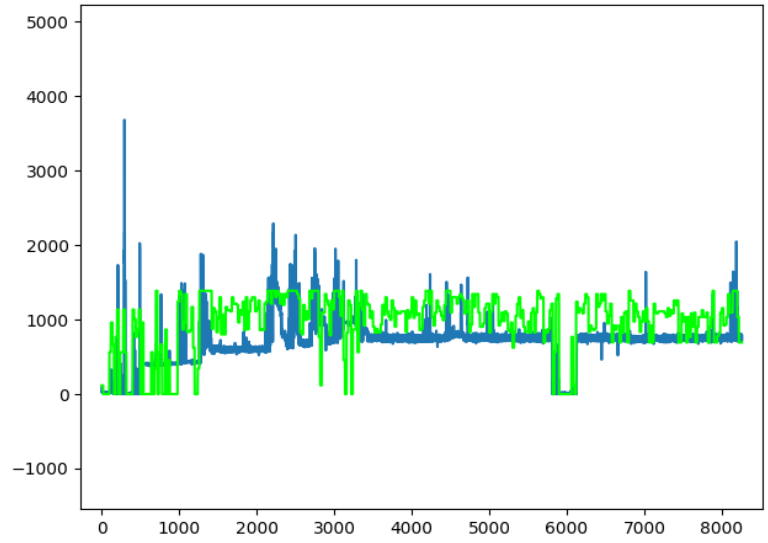
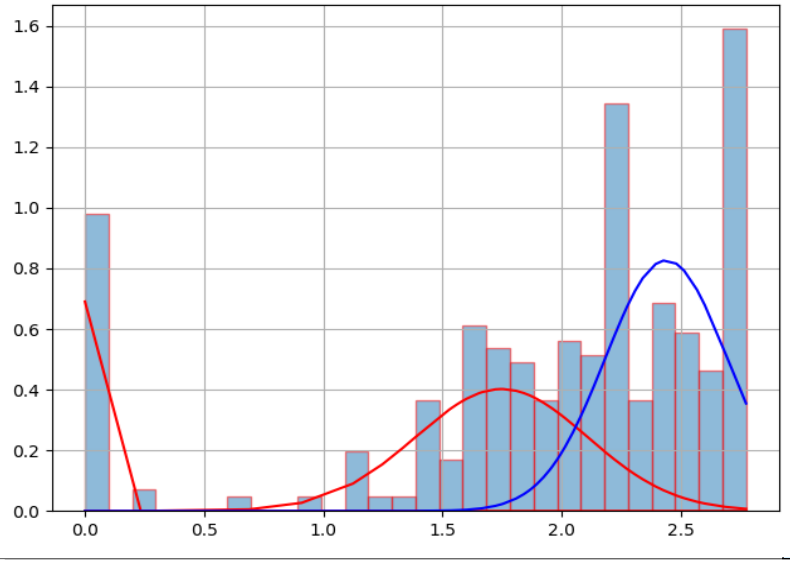
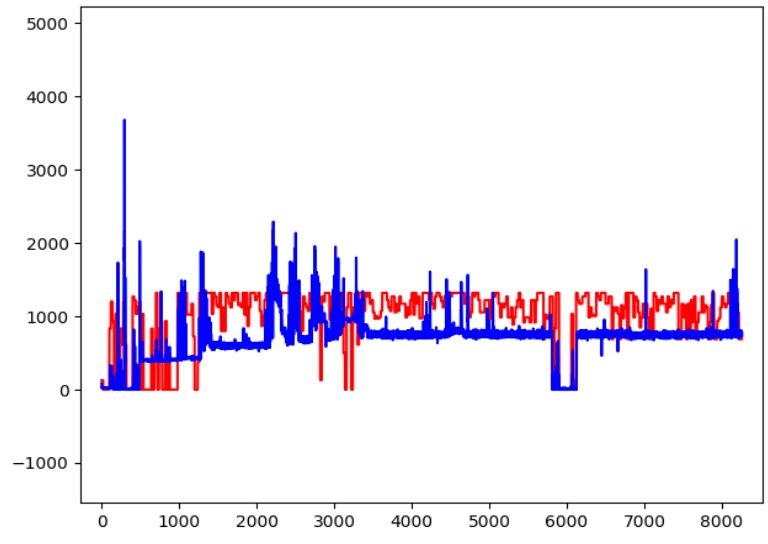
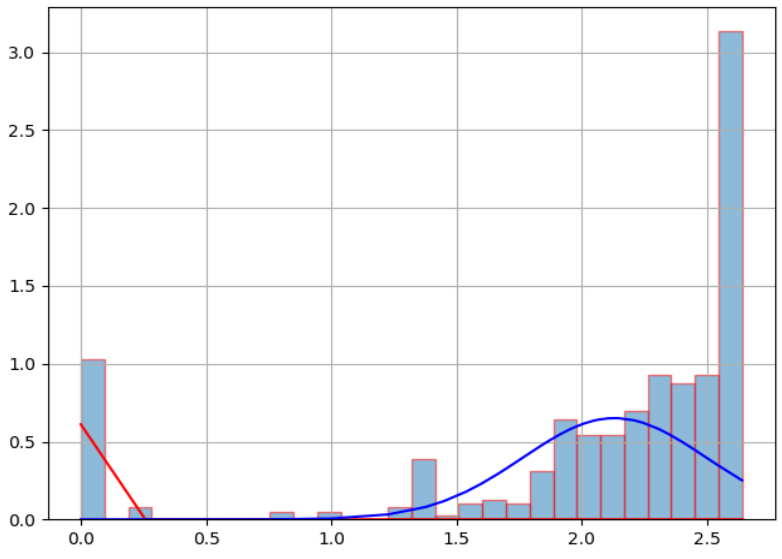
Пара-метры	Временной и энтропийный ряды	Гистограмма и параметры смешанного распределения	Исходн данные
Интер-вал 50 Окно 2			*m*: 0; 1.23; 2.29. D: 0.13; 0.09; 0.
Интер-вал 50 Окно 3			*m*: 0; 1.58; 2.48. D: 10^{-6}; 0.15; 0.12.

Таблица 7 – Модельный пример (продолжение)

Пара-метры	Временной и энтропийный ряды	Гистограмма и параметры смешанного распределения	Исходн данные
Интер-вал 50 Окно 5			*n*: 0.02; 1.70; 2.41. *D*: 0.07; 0.003; 0.12.
Интер-вал 50 Окно 7			*n*: 0.01; 2.13; 2.63. *D*: 10^{-5}; 0.01; 0.1.

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

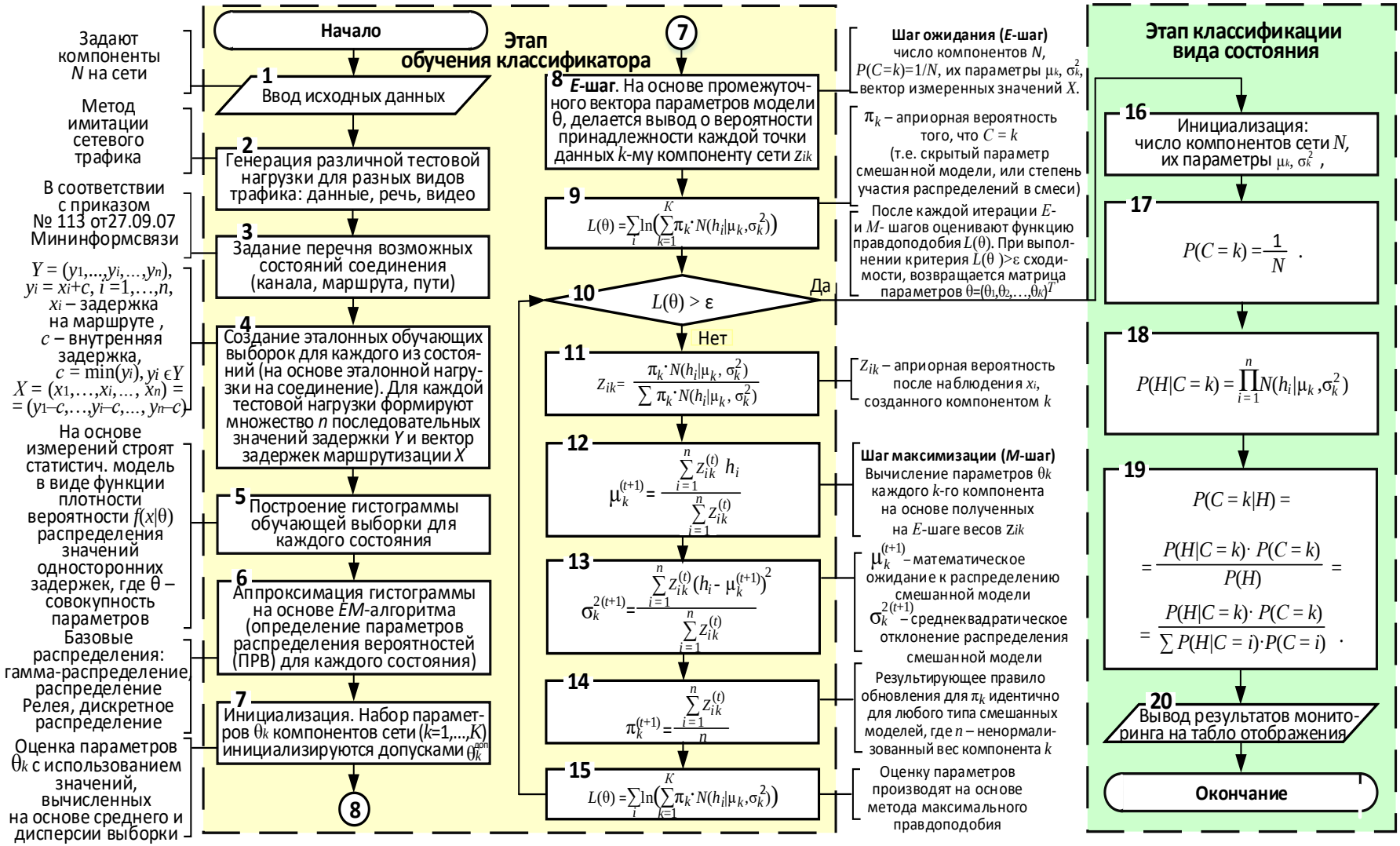


Рис. 21. Обучение классификатора с использованием *EM*-алгоритма и классификация вида состояния

8.4. Алгоритм превентивной идентификации аномального состояния сетевого элемента на временных рядах его метрик

Исходя из рассмотренных методов анализа временных рядов предложен алгоритм превентивной идентификации аномального состояния сетевого элемента на временных рядах его метрик. Блок-схема алгоритма состоит из четырех этапов: предварительного этапа, этапа кодирования временных рядов, этапа идентификации состояния сетевого элемента и завершающего этапа, рис. 22.

Предварительный этап

Ввод исходных данных: о составе ИТКС; структуре ее децентрализованной подсистемы мониторинга (матрица тяготений серверов мониторинга к сетевым элементам); наблюдаемых параметрах сетевых элементов; величинах эксплуатационных допусков на параметры сетевых элементов, а также значениях профилактических допусков на них для различных режимов функционирования и условий эксплуатации сетевых элементов [67]; режимах мониторинга (активный, пассивный) и периодичности опроса сервером мониторинга сетевых элементов; значениях ошибок первого и второго рода (α – «ложной тревоги» и β – «пропуск отказа», соответственно); видах технического состояния сетевого элемента; используемых протоколах сбора измерительной информации и др.

Первоначальное назначение серверам мониторинга сетевых элементов для наблюдения их ТС (мониторинга) в соответствии с матрицей тяготения серверов к сетевым элементам из расчета охвата каждого сетевого элемента не менее чем двумя серверами мониторинга.

Определение мощности алфавита кодирования временного ряда с разбиением диапазона размаха варьируемых значений метрики на сегменты, соответствующие классам (видам) технического состояния сетевых элементов, закрепляемые за символами кода. Соотнесение классов (видов) ТС [7] с символами выбранного алфавита Σ кодирования временного ряда.

Выбор размера скользящего окна (по методике Сметанина Ю.Г., Ульянова М.В. [65] и др.). Для каждого эксплуатационного параметра отдельного сетевого элемента данный выбор индивидуален. Важно ширину скользящего окна иметь таковой, чтобы не пропустить нарастание аварийной ситуации в различных режимах и условиях эксплуатации сетевого элемента, а также минимизировать ошибки первого рода (α) «ложный отказ» и второго рода (β) «пропуск отказа». Выбор размера скользящего окна, как правило, осуществляется на этапе испытаний или подконтрольной эксплуатации сетевого элемента. А процедура минимизации ошибок первого и второго рода является самостоятельной оптимизационной задачей.

Введение запрещенных слогов на наблюдаемом кодовом слове-строке, приводящих к отказу. Первоначально состав запрещенных слогов определяется в ходе испытаний и подконтрольной эксплуатации для различных режимов функционирования и условий эксплуатации сетевого оборудования, а в последующем – в соответствии нарабатываемой статистикой на основных этапах жизненного цикла ИТКС. Поэтому этапу испытаний и подконтрольной эксплуатации должно уделяться важное значение.

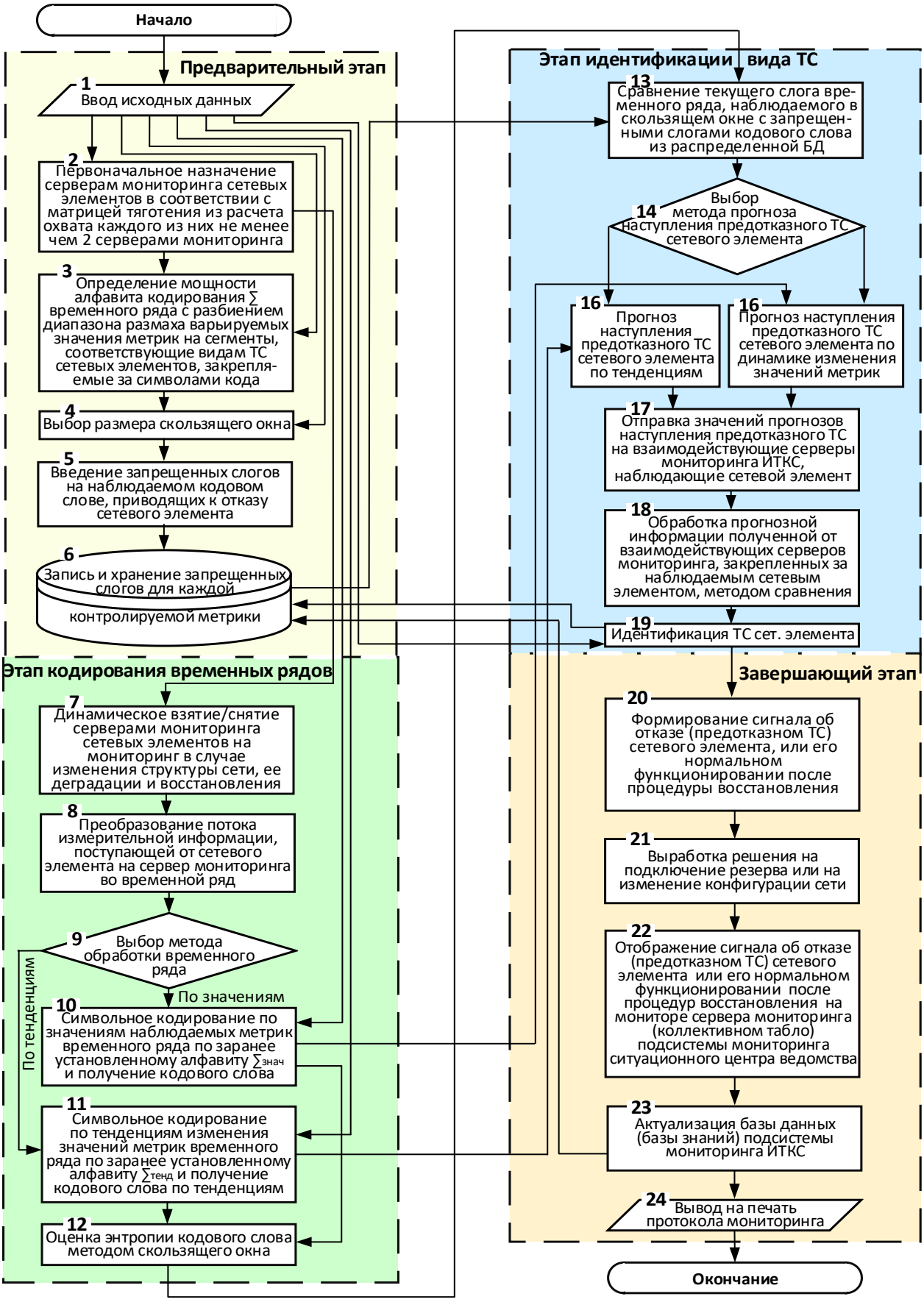


Рис. 22. Блок-схема алгоритма превентивной идентификации аномального состояния сетевого элемента на временных рядах его метрик

Запись и хранение запрещенных слогов для каждой контролируемой метрики каждого сетевого элемента в распределенной базе данных (базе знаний – БЗ) ИТКС, их обновление и репликация в соответствии с надежностью функционирования ИТКС и статистикой эксплуатации сетевых элементов на основных этапах их жизненного цикла.

Этап кодирования временных рядов

Динамическое взятие/снятие серверами мониторинга сетевых элементов на мониторинг в случае изменения структуры сети, ее деградации или восстановления, из расчета охвата каждого сетевого элемента не менее чем двумя серверами мониторинга Такое динамическое распределение одновременно должно модифицироваться любым из участвующих серверов для поддержки выполнения условия обеспечения $\sum_{i=1}^{M_{\max}} m_i \geq 2$ минимального количества серверов мониторинга (не менее двух) на одно сетевое устройство.

Преобразование потока ИИ, поступающей от сетевого элемента в сервер мониторинга во временном ряду, а также выбор вида временного ряда и типа средств его визуализации.

Выбор метода обработки временного ряда – символьное кодирование по значениям или символьное кодирование по тенденциям.

Символьное кодирование значений наблюдаемых метрик временного ряда в соответствие с символами ранее установленного алфавита $\Sigma_{\text{знач}}$ и получение кодовых слов-строк по значениям.

Символьное кодирование по тенденциям изменения значений метрик временного ряда символами ранее установленного алфавита $\Sigma_{\text{тенд.}}$ и получение кодовых слов-строк по тенденциям.

Оценка энтропии кодового слова. Изначально позиционированное в начале наблюдаемого кодового слова-строки длиной n, скользящее окно шириной m сдвигается каждый раз на один символ (временной такт) t_{i+1}. Для каждого его $n - m + 1$ положения распознается слог кодового слова, полученный в скользящем окне. Если в текущей позиции скользящего окна шириной m наблюдается слог, имеющий номер i в принятой нумерации, то значение счетчика c_i увеличивается на единицу. Расчет оценки энтропии слов C_m проводится по выражению (1).

Этап идентификации состояния сетевого элемента

Сравнение текущего слога временного ряда, наблюдаемого в скользящем окне с запрещенными слогами кодового слова, записанными в распределенной БД (БЗ) предполагает поиск (фильтрацию) запрещенных слогов в наблюдаемом кодовом слове-строке временного ряда.

Выбор метода прогноза наступления предотказного ТС сетевого элемента.

Прогноз наступления предотказного состояния сетевого элемента *по тенденциям* их изменения (выявление опасных тенденций). В случае идентификации опасных трендов развития аварии необходимо увеличить частоту опроса сетевого элемента с целью не допустить пропуска отказа и минимизировать ошибку второго рода β. В данном алгоритме процедура увеличения скважности опроса сетевого элемента серверов мониторинга при выявлении предотказного

технического состояния не представлена, решается программно отдельным блоком алгоритма.

Прогноз наступления предотказного состояния сетевого элемента по динамике изменения *значений* метрик в наблюдаемых слогах ключевых слов анализируемого ряда временного ряда. В случае идентификации предотказного технического состояния сетевого элемента доступная измерительная информация (величины значений наблюдаемой метрики) сверяется не только с эксплуатационным допуском на параметр, но и с профилактическим допуском, зависящим от конкретного режима функционирования и условий эксплуатации сетевого элемента.

Отправка значений прогнозов наступления предотказного технического состояния на серверы мониторинга, взаимодействующие в ИТКС и наблюдающие сетевой элемент. При этом если на сервере мониторинга, спрогнозировавшим предотказное состояние доступна измерительная информация инструментального контроля, то на взаимодействующие серверы мониторинга передается только прогнозное значение в виде символьной записи (типа {+ + +}, или {*ABE*}).

Обработка прогнозной информации, полученной на шагах прогноза и поступающей от взаимодействующих серверов мониторинга ИТКС, закрепленных за наблюдаемым сетевым элементом, методом сравнения (с использованием мажоритарного принципа и пр.), а также сопоставления действующих режимов его функционирования и условий эксплуатации (выявление причин наступления предотказного состояния).

Идентификация технического состояния сетевого элемента по конечному символу текущего слога наблюдаемого кодового слова временного ряда.

Завершающий этап

Формирование сигнала об отказе, предотказном ТС или иной аномалии сетевого элемента, или его нормальном функционировании после процедур восстановления (устранения отказа).

Выработка решения на подключение резерва или на изменение конфигурации сети в связи с отказом/восстановлением сетевого элемента. Для повышения оперативности доведения оповещения до системы поддержки принятия решения данный шаг выполняется параллельно с предыдущим.

Отображение сигнала об отказе (предотказном ТС) сетевого элемента или его нормальном функционировании после процедур восстановления (устранения отказа) на мониторе сервера мониторинга (коллективном табло) подсистемы мониторинга.

Актуализация базы данных (базы знаний) о ТС сетевых элементов ИТКС, обновление структуры сети в связи с последними изменениями (отказом, резервирование, восстановлением), динамическое перезакрепление серверов мониторинга за сетевыми элементами в связи с динамикой изменения ТС ИТКС (изменение матрицы тяготения серверов мониторинга и сетевых элементов), уточнение исходных данных, обновление и репликация распределенной БД ИТКС.

Вывод на печать протоколов мониторинга.

№4. 2021
ISSN 2410-9916

Результаты эксперимента

Описанный в методике подход с классификацией состояния элементов телекоммуникационной сети неплохо работает в случае возможности выделения классов поведений. Это было продемонстрировано для односторонней задержки [60], когда компонента, связанная с маршрутизацией (ожидание в очередях), включается в общее выражение задержки лишь при средних и высоких нагрузках. В меньшей степени этот метод может быть использован для оценки состояния загрузки вычислительных ресурсов, в частности процессора. Хотя и здесь имеет место задержка, связанная с переключением контекста вычисления, но она более связана с организацией вычислительного процесса, чем с режимом нагрузки. В этом случае требуется предварительный этап уточнения числа состояний и соответствующих им распределений.

Это было продемонстрировано в ходе выполненного эксперимента, результаты которого приведены на рис. 23 и 24.

Проведя анализ аппроксимации гистограмм загрузки процессора несколькими распределениями выбранных параметров, можно сделать вывод, что наиболее информативна аппроксимация гистограмм наблюдаемых параметров (метрик) сетевых устройств, с двумя нормальными распределениями.

Эксперимент проводился на гистограммах статистики недельной загрузки процессора сервера виртуализации двумя и тремя нормальными распределениями по смешанной гауссовской модели *EM*-алгоритмом. Гистограммы были получены на том же наборе данных, что было использовано для установления оптимальной величины окна для расчета энтропии сдвигов. Как следует из рисунков, предобработка данных энтропией сдвигов позволяет «разнести» распределения, моделирующие состояния, что обеспечивает более точную их классификацию. При этом хорошо видно, что две компоненты обеспечивают более точную классификацию технического состояния сетевого устройства (рис. 23), нежели три (рис. 24). Эксперимент проводился на параметрах загрузки процессора (тактах).

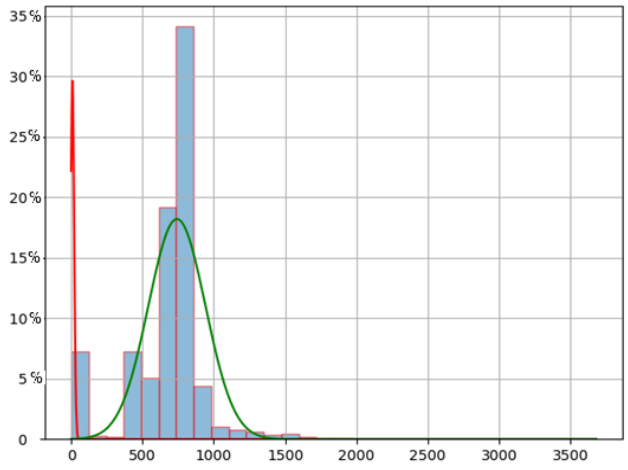


Рис. 23. Аппроксимация гистограммы загрузки процессора двумя нормальными распределениями

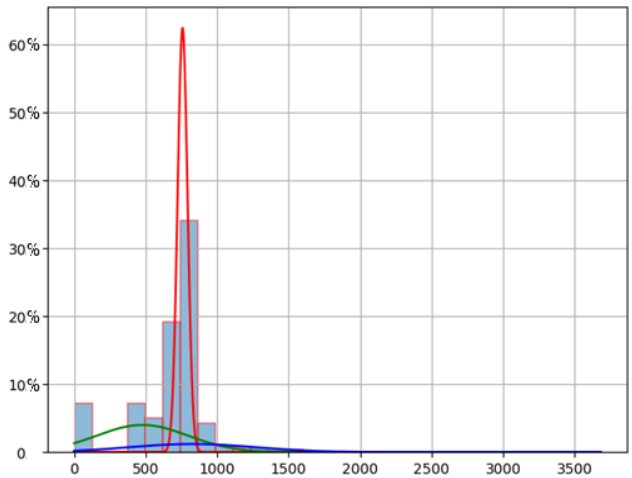


Рис. 24. Аппроксимация гистограммы загрузки процессора тремя нормальными распределениями

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

9. Методы анализа состояния сетей и соединений: каналов, маршрутов, путей

9.1. Выбор показателей качества (метрик) системы мониторинга ИТКС. Что мониторить?

При ответе на вопрос что будем мониторить, перспективной системе мониторинга при оценке состояния ИТКС ОП следует руководствоваться оптимальностью изначального выбора первичных измеряемых параметров, которые затем агрегируются процедурами вычисления интегральных сетевых метрик. При решении этой задачи оптимальность должна заключаться как в количестве первичных параметров сети, так и в числе измерений (скважности опроса сервером мониторинга сетевых элементов). Иначе анализ измерительных выборок может занимать слишком большое количество времени, а каналы связи будут перегружаться потоками измерительной информации (например, при опросе сетевых элементов каждую секунду, или каждые 5-10 с), что неминуемо приведет к нарушению требований относительно скорости реакции системы управления. Конечно же, для ИТКС КВИ, например, объектов атомной энергетики, такая высокая скважность опроса объектов мониторинга оправдана. В таких инфраструктурах и каналы контроля являются специально выделенными. В то же время в ИТКС ОП, как правило, для систем мониторинга используется тот же канальный ресурс, что и для передачи основного трафика (данные, видео, голос).

При выборе показателей качества системы мониторинга следует учитывать требования:

– по точности, предъявляемой к системе сетевого мониторинга;
– вычислительным мощностям подсистемы анализа данных;
– разрешающей способности средств сбора первичных параметров (сырых данных).

Делая подобный выбор показателей качества систем мониторинга ИТКС, можно исходить из некоторой абстрактной модели, адекватно отражающей различные аспекты функционирования сети. В качестве модели, отражающей динамику функционирования сети, используем модель сети массового обслуживания (СМО), предложенную в [71].

Представим сеть на некотором уровне (сетевом уровне OSI) в виде неориентированного графа, вершинами которого служат обрабатывающие приборы (маршрутизаторы и хосты), а соединяющие их дуги – каналы, которые характеризуются используемой технологией канального уровня модели OSI (Ethernet, Token Ring, Frame Relay и пр.). Тогда под маршрутом понимается некоторый путь в графе сети.

Основой при описании задач управления конфигурацией и производительностью является концепция достаточности ресурса. Согласно [72] под ресурсом подразумевают *средства*, которые позволяют с помощью определённых преобразований получить желаемый *результат*.

В качестве результата при построении (синтезе) перспективной системы мониторинга выступает передача сигналов телеизмерения-телесигнализации

(ТУ-ТС) от источника к узлу назначения и обратно. При этом сервер мониторинга генерирует запросы (сигналы телеуправления – ТУ), а объект мониторинга – ответы в виде значений измеренных параметров сетевого элемента (сигналы телесигнализации – ТС). В некоторых телеизмерительных системах и системах контроля данные сигналы называют сигналами телеизмерения (ТИ).

В связи с тем, что все перечисленные сигналы используют один и тот же канальный ресурс ИТКС, а следовательно в основе их лежит одна модель канала с его параметрами и вероятностно-временными характеристиками (ВВХ), независимо от изотропности канала связи (от направления передачи потоков управляющей и измерительной информации), то в данной работе сигналы ТУ-ТС будем называть измерительной информацией (ИИ), или данными.

Исходя из этого, привязываясь к определению ресурса [72], в качестве результата в данной работе (в системе мониторинга) выступают потоки измерительной информации, а средствами, с учетом принятых допущений – пропускные способности каналов и процессорное время обрабатывающих элементов системы мониторинга.

При этом многочисленные публикации [73, 74 и др.] показали, что для большинства систем накладные расходы операционной системы и протокола мониторинга составляют основное время задержки сетевой операции, а иногда удвоение производительности процессора приводит к удвоению пропускной способности выбранного маршрута на сети.

Кроме перечисленных показателей качества, характеризующих конкретное распределение ресурсов (*метрики использования ресурсов*), особый интерес представляют метрики, которые показывают степень влияния этого проведенного распределения на производительность (*метрики производительности*), на клиента некоторого прикладного сервиса (*метрики готовности*) и на стабильность (устойчивость) ИТКС в целом (*метрики стабильности*).

Исходя из сказанного, в таблице 8 представлены описываемые в работе группы метрик для мониторинга ИТКС ОП, а в таблице 9 приведены группы метрик для мониторинга сетевых устройств (на примере IP-сети):

– метрики использования ресурсов;
– метрики производительности системы;
– метрики готовности системы;
– метрики стабильности.

9.2. Выбор методов измерений системы мониторинга ИТКС. Как мониторить?

При ответе на вопрос как будем мониторить информационно-телекоммуникационную сеть необходимо рассмотреть методы проведения измерений и сбора измерительной информации с объектов контроля в интересах серверов мониторинга перспективной системы мониторинга.

В таблице 10 приведены наиболее применимые методы проведения измерений на ИТКС ОП (на примере IP-сети).

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

Таблица 8 – Группы метрик системы мониторинга ИТКС ОП (на примере IP-сети)

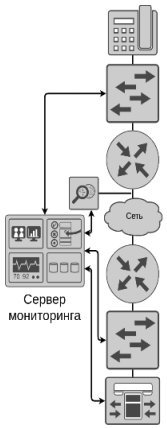
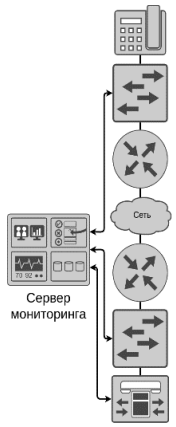
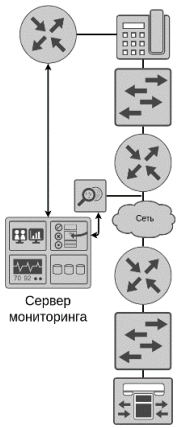
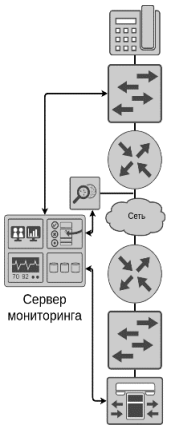
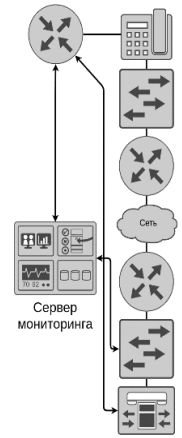
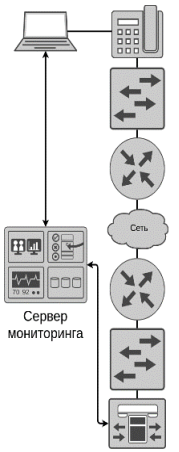
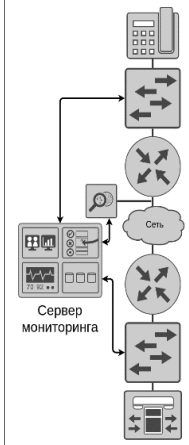
Метрики использования ресурсов			
Счетчик IS MIB	**Метрики пропускной способности канала**	**Параметры**	**Расчетные соотношения**
ifInOctets	полное число полученных октетов	Коэффициент использования ресурса (КИ) Δt – временной интервал, через который производится измерен. параметров; $\Delta ifInOctets$ – количество октетов, полученных из канала интерфейсом за время Δt; $\Delta ifOutOctets$ – количество октетов, переданных в канал интерфейсом за время Δt; *ifSpeed* – скорость, характеризующая используемую технологию канального уровня (Бит/сек)	$КИ = r/R$, где r – часть используемого ресурса, R – объем имеющегося ресурса. $ifInOctets = ifOctets(t+\Delta t) - ifOctets(t)$ *a*) Для полудуплексного канала: $КИ_{half} = \frac{\Delta ifInOctets + \Delta ifOutOctets}{t * ifSpeed} * 8 * 100$. *b*) Для полнодуплексного канала: $КИ_{full} = \frac{max(\Delta ifInOctets, \Delta ifOutOctets)}{t * ifSpeed} * 8 * 100$; $КИ_{in.} = \frac{\Delta ifInOctets}{\Delta t * ifSpeed} * 8 * 100$; $КИ_{out} = \frac{\Delta ifOutOctets}{\Delta t * ifSpeed} * 8 * 100$.
ifOutOctets	полное число переданных октетов		
ifInUcastPkts	полное число полученных unicast-пакетов		
ifOutUcastPkts	полное число переданных unicast-пакетов		
ifInNUcastPkts	число полученных мультикастинг- и широковещательных пакетов		
ifOutNUcastPkts	число переданных мультикастинг- и широковещательных пакетов		
ifInDiscards	число полученных, но отвергнутых пакетов		
ifOutDiscards	количество отвергнутых пакетов из числа отправленных		
ifOperStatus	текущее состояние интерфейса: 1 – вкл; 2 – выкл; 3 – тест		
sysUpTime	системное время		
Метрики производительности (Рек. ITU-T: Y.1540 [75], M.2301 [76])			
	Задержка	Задержка передачи *IP*-пакетов (*IPTD*) определяется для всех успешных и ошибочных исходов пакетов в базовом разделе или *NSE*. *IPTD* – это время (t_2–t_1) между возникновением двух соответствующих событий ссылки на *IP*-пакет, входящего события $IPRE_1$ в момент времени t_1 и выходного события $IPRE_2$ в момент времени t_2, где ($t_2 > t_1$) и ($t_2 - t_1$) $\leq T_{max}$. *IPER* – это отношение общего числа исходов *IP*-пакетов с ошибками к успешным исходам. *IPLR* – это отношение общего количества потерянных результатов *IP*-пакетов к общему количеству переданных *IP*-пакетов. *Bandwith* – максимальная скорость передачи данных в сети в определенный момент времени по определенному соединению.	Для каждой метрики протокол *OSPF* строит отдельную таблицу маршрутов, выбор которой происходит в зависимости от значений битов *TOS* в заголовке пришедшего пакета. Если бит $D = 1$ (*Deley* – задержка) – маршрут выбирают из таблицы маршрутов, минимизирующих задержку. Если бит $T = 1$ (*Throughput* – пропускная способность – ПС) – – маршрут выбирают из таблицы маршрутов, построенной с учетом пропускной способности,. Если бит $R = 1$ (*Reliability* – надежность) – маршрут выбирают из таблицы маршрутов, оптимизирующих надежность доставки
One-Way Delay (*OVD*)	односторонние задержка (*OWD*)		
IP packet transfer delay (*IPTD*)	задержка передачи *IP* пакета (*IPTD*)		
IP packet delay variation (*IPDV*)	отклонение задержки *IP* пакетов (*IPDV*)		
	Надежность передачи пакетов		
IP packet error ratio (*IPER*)	коэффициент ошибок в *IP* пакетах (*IPER*)		
IP packet loss ratio (*IPLR*)	коэффициент потери *IP*-пакетов (*IPLR*)		
IP packet reordered ratio (*IPRR*)	коэффициент изменения порядка следования *IP* пакетов (*IPRR*)		
	Полоса пропускания соединения		
bandwith	ширина полосы пропускания (*bandwith*)		
Метрики готовности			
Коэффициент готовности (КГ) $КГ = \frac{MTBF}{MTBF + MTTR}$	Это мера способности сервера предоставлять клиентам ресурсы. Измеряется в процентах времени, проведенном системой в работоспособном состоянии, от всего времени работы.	*MTBF* – средняя наработка на отказ (mean time between failures) *MTTR* – среднее время восстановления (mean time to repair)	$КГ = \frac{количество\ принятых\ ping\text{-}запросов}{количество\ посланных\ ping\text{-}запросов} * 100$; $КГ = \frac{количество\ полученных ответов}{количество\ посланных\ запросов} * 100$
Метрики стабильности (Рек. IETF RFC 3393)			
Вариация задержки (джиттер)	Интегральный показатель переходных процессо в сети. Постоянные и кратковременные флуктуации	Джиттер – есть разница между значениями односторонних сетевых задержек (*OWD*) при двух последовательных измерениях	$j = \frac{1}{n-1} \sum_{i=1}^{n-1} \left\| D_{i+1} - D_i \right\|$, где D_i и D_{i+1} – значения двух последовательных измерений *OWD*

Таблица 9 – Группы метрик системы мониторинга сетевых устройств (на примере IP-сети)

Метрики использования ресурсов Коэффициент использования ресурса (КИ) – отношение части используемого ресурса *r* к объему имеющегося ресурса *R*: ***КИ = r/R***			
Счетчик *Internet Standard MIB*	**Описание метрик пропускной способности устройства (*для стандартного агента SNMP*)**	**Параметры**	**Расчетные соотношения**
ssCpuRawUser	число "тактов" процессора, отведенных под программы (код) пользовательского уровня		$ssCpuRaw = ssCpuRawIdle + ssCpuRawNice + ssCpuRawWait + ssCpuRawKernel + ssCpuRawInterrupt$ $КИ_{проц} = \frac{ssCpuRaw - ssCpuRawIdle}{ssCpuRaw} = 1 - \frac{ssCpuRawIdle}{ssCpuRaw}$
ssCpuRawNice	число "тактов" процессора, отведенных под программы (код) с пониженным приоритетом		
ssCpuRawSystem	число "тактов" процессора, отведенных под программы (код) системного уровня		
ssCpuRawIdle	число незадействованных "тактов" процессора		
ssCpuRawWait	число "тактов" процессора, отведенных под ожидание ввода-вывода (*IO*) (*system-level code*)		
ssCpuRawKernel	число "тактов" процессора, отведенных программы (код) уровня ядра (*kernel-level code*)		
ssCpuRawUser	число "тактов" процессора, отведенных под обработку аппаратн. прерыван. (*hardware interrupts*)		
Метрики производительности			
Переменная *Internet Standard MIB*	**Описание метрик производительности устройств**	**Параметры**	**Расчетные соотношения**
ipInReceives	общее число полученных интерфейсом пакетов	Число пакетов за интервал времени Δt, $\Delta ipInReceives$–полученных интерфейсом; $\Delta ipInDelivers$–полученных без ошибок; $\Delta ipInHdrErrors$ –отвергнутых из-за ошибок; $\Delta ipInAddrErrors$ – отвергнутых из-за неправильного адреса; $\Delta ipInDiscards$ – отвергнутых из-за отсутствия буферной памяти $\Delta ipForwDatagrams$ – транзитных пакетов-*Datagram*	$KT_{ip} = \frac{\Delta ifInDelivers}{\Delta IPInReceives} * 100;$ $f_{ipHdrErr} = \frac{\Delta ipInHdrErrors}{\Delta ipInReceives};$ $f_{ipAddrErr} = \frac{\Delta ipInAddrErrors}{\Delta ipInReceives} * 100;$ $f_{ipDiscards} = \frac{\Delta ipInDiscards}{\Delta ipInReceives};$ $f_{ipForwDat} = \frac{\Delta ipForwDatagrams}{\Delta ipInReceives} * 100$
ipInHdrErrors	число отвергнутых пакетов из-за ошибок, истекло *TTL*		
ipInAddrErrors	число отвергнутых пакетов из-за неверного *IP* адреса		
ipForwDatagrams	число транзитных (по маршруту) пакетов-*Datagram*		
ipInUnknownProtos	число пакетов с неподдерживаемым кодом протокола		
ipInDiscards	число пакетов, отвергнутых из-за переполнения буфера		
ipInDelivers	полное число входных пакетов, успешно обработанных		
Метрики готовности			
Коэффициент готовности (КГ)	Мера способности сервера предоставлять клиентам ресурсы. КГ обычно измеряется в процентах времени, проведенном системой в работоспособном состоянии, от общего времени работы.	*MTBF* – средняя наработка на отказ (mean time between failures) *MTTR* – ср. время восстановления (mean time to repair)	$КГ = \frac{количество\ принятых\ ping - запросов}{количество\ посланных\ ping - запросов} * 100;$ $КГ = \frac{количество\ полученных\ ответов}{количество\ посланных\ запросов} * 100$ $КГ = \frac{MTBF}{MTBF + MTTR}$
Метрики стабильности			
Вариация задержки (джиттер)	Интегральный показатель переходных процессов в сети. Постоянные и кратковременные флуктуации	Джиттер – есть разница между значениями односторонних сетевых задержек (*OWD*) при двух последовательных измерениях	$j = \frac{1}{n-1} \sum_{i=1}^{n-1} \left\| D_{i+1} - D_i \right\|,$ где D_i и D_{i+1} – значения двух последовательных измерений односторонних сетевых задержек для выбранного сетевого маршрута

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

Таблица 10 – Методы проведения измерений на ИТКС ОП (на примере IP-сети)

Методы проведения измерений				**Методы сбора измерительной информации**			
Пассивные методы		*Активные методы*		*Встроенные агенты*		*Внешний метод сбора*	
	Используется реаль-ный трафик. Измеря-ются временные пара-метры трафика, генери-руемого приложения-ми. Как следствие, дос-таточно точное измере-ние. **Недостатки:** ограниченный спектр типов трафиков, которые не всегда представлены в реальной ситуации. Прогноз, построенный на основе данных измерения точен лишь на малом интервале, пока не появятся новые приложения, услуги, изменяющие трафик.		Специально генери-руемый трафик для целей измерения па-раметров производи-тельности сети. **Пре-имущества:** измере-ние проводится меж-ду двумя точками сети и является конт-ролируемым. Трафик специального класса, устанавливаемого при помощи поля *IP-precedence* в *IP*-пакеах. **Недостатки:** генерируемый тра-фик является лишь аппроксимацией реального трафика.		Механизмы сбора ста-тистики интегриро-ваны в устройства (маршрутизаторы, коммутаторы и пр.). **Преимущества**: соот-ветствует сетевой ин-фраструктуре, позво-ляет измерять параме-тры, измерение кото-рых невозможно при внешнем сборе стати-стики (очевидно *Real Time*). **Недостатки:** ориентация методов измерения произво-дительности на устро-йства, а не их агрега-ции и совокупности.		Механизмы сбора ста-тистики интегриро-ваны в специализиро-ванное устройство, специально предназ-наченное для измере-ния параметров про-изводительности. **Преимущества**: из-мерение параметров производится незави-симо от устройств, передающих трафик. **Недостатки**: область измерения (в смысле геогра-фии) ограни-чена. Статистики измеряются только в точках подключения.
Ориентация измерения				**Цель измерения**			
Устройство/линк		*Точка-точка*		*Пользователь*		*Сеть*	
	Измерение производите-льности сети проводится на основе исследования отдельных устройств, ин-терфейсов и обычно осно-вывается на частотном анализе использования тех или иных ресурсов устройств. **Преимущества**: деталь-ный мониторинг параме-тров функционирования критичных устройств. **Недостатки:** сложность или невозможность декомпозиции и сведения возникающих в сети сбоев к сбоям одного устройства		Метод измерения осно-вывается на време-ни отклика участка, состоящего из одного или нескольких уст-ройств и зачастую основывается на измерениях задержек (разных). **Преимущества**: отражение действиите-льного состояния учас-тка (не модельное). **Недостатки**: для принятия решения все равно необходи-мо знание о количест-венном и качествен-ном составе участка.		Измерения основываются на статистиках производительности, собранных непосредственно на рабочем месте пользователя. **Преимущества:** точное измерение действительного уровня производительности с точки зрения конечного пользователя. **Недостатки**: может влиять на работу пользователя.		Измерение основы-вается на сборе ста-тистик с отдельных сетевых элементов. **Преимущества**: простота развертывания, не влияет на работу пользователя, полное описание параметров производительности **Недостатки:** несо-вершенное (урезан-ное) представление о параметрах произ-водительности со стороны конечного пользователя.

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

9.3. Методы анализа состояния сетей и соединений (каналов, маршрутов, путей)

Приведенный выше анализ современных систем мониторинга ИТКС ОП показывает, что в рамках данных систем, главным образом реализуется мониторинг сетевых элементов. Каждый цикл опроса сетевого элемента сводится к выполнению проверки его доступности, опросу структурных (маршрутные таблицы) и динамических (уровни загрузки ресурсов, частота ошибок) характеристик. Уровень сетевого управления, рассматривающий поведение сетевых элементов во взаимосвязи, реализуется, как правило, как часть функции мониторинга отказов (fault management) в задачах корреляции и фильтрации неисправностей (event correlation). Как известно, это предполагает использование априорно заданных моделей, описывающих взаимное влияние устройств. Наиболее часто для решения данной задачи используются модели на основе правил (rule-based evet correlation), описывающих взаимное влияние в виде «Если вышло из строя устройство *A*, то *B* и *C* будут недоступны». В случае выхода из строя *A*, в журнале проверок элементов будет наблюдаться три события: *A, B, C*. Применив данное правило мы сможем определить, что первопричиной отказа является именно *A*.

Составление подобного множества правил корреляции требует от обслуживающего персонала досконального знания сети, что в случае большого ее размера представляет собой сложную задачу. К тому же любые структурные изменения (например, добавление нового элемента) в сети будут требовать изменение множества правил.

В данной работе, согласно циклу работ [77] представлен обзор двух групп методов, учитывающих взаимное влияние сетевых элементов в динамике: методы сетевой томографии; методы на основе расстояния редактирования графов.

9.3.1. Методы сетевой томографии

Основную идею сетевой томографии лучше всего продемонстрировать на примере. Допустим, что проводится измерение на сети (рис. 25 а). В составе сети 4 узла *A, B, C, D*. Для того, чтобы установить состояние каждого из соединений *A-B, B-C* и *C-D* достаточно выполнить 2 измерения *A-C* и *A-D*. В случае, если выйдет из строя *A-B* оба маршрута *A-C* и *A-D* будут недоступны для передачи. Если выйдет из строя *B-C*, то *A-C* будет недоступен, а *A-D* будет функционировать. То же верно и для *B-D*. Аналогично, выполнив 4 измерения *A-E, A-F, D-E* и *D-F* на структуре представленной на рис. 25 *b*), можно охарактеризовать каждый из пяти каналов. Таким образом, для установления факта выхода из строя соединения необходимо, чтобы через данное соединение проходило 2 маршрута, по которым проводится измерение, и чтобы эти 2 измерения были отрицательны (т. е. передача по данному маршруту была в данный момент невозможна).

В настоящее время предложены методы дискретной (булевской) томографии и непрерывной томографии. В булевской томографии каждое соединение предполагается в состоянии «работает» или «не работает». Приведенный выше пример соответствует данному виду томографии.

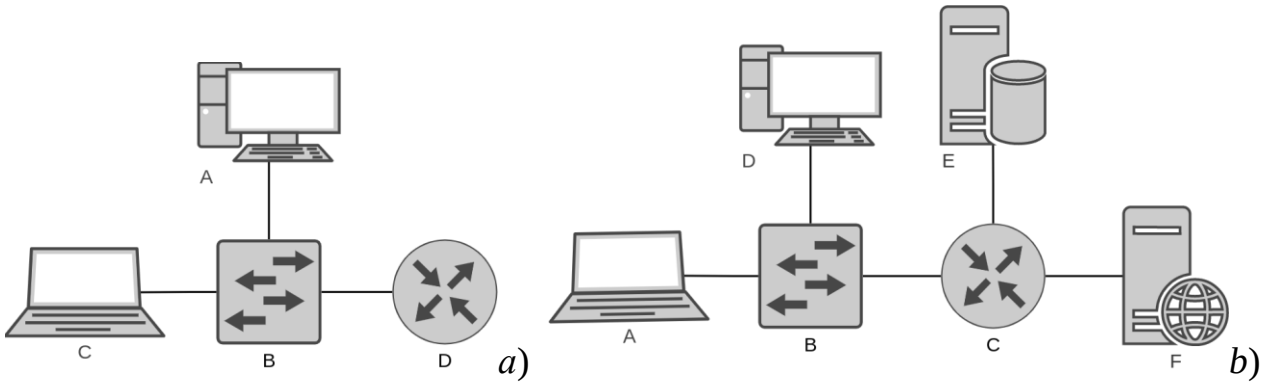


Рис. 25. Пример структур сетей, состояние каналов которых может быть реконструировано средствами сетевой томографии

Второй вид томографии предполагает, что соединение характеризуется распределением вероятностей. В этом случае путь (последовательность соединений) характеризуется смешанным распределением вероятностей, и задача реконструкции решается упомянутым *EM*-алгоритмом.

В настоящее время методы сетевой томографии не получили распространения вследствие вычислительной сложности (непрерывный случай), вопросов по устойчивости результатов и необходимости создания достаточной инфраструктуры измерения, что не всегда возможно на существующей сети.

9.3.2. Методы на основе расстояния редактирования графов

Очевидной формой представления ИТКС ОП являются графы. Узлы сети, которыми могут быть группы пользователей или отдельные клиенты и серверы, представляются вершинами графа (множество V), а дуги графа (множество E) представляют логические связи, например направления связи или маршруты передачи данных между узлами. Граф $g = (V, E, \alpha, \beta)$, описывающий сеть предполагает также наличие функции разметки узлов α: $V \rightarrow L_V$, которую, будем считать инъективной: $\alpha(x) = \alpha(y)$ только в случае, если $x = y$. В качестве меток вершин будем предполагать уникальные идентификаторы узлов. Задание графа предполагает наличие функции разметки ребер β: $E \rightarrow L_E$. В качестве меток ребер может быть использован набор следующих характеристик:

– ширина полосы пропускания (максимальное, минимальное, среднее);
– односторонняя задержка (максимальное, минимальное, среднее);
– объем переданных данных.

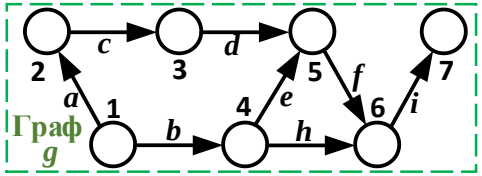
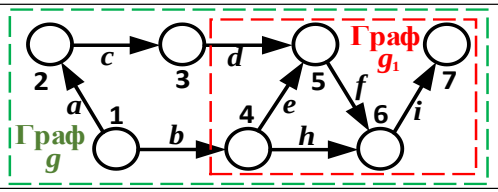
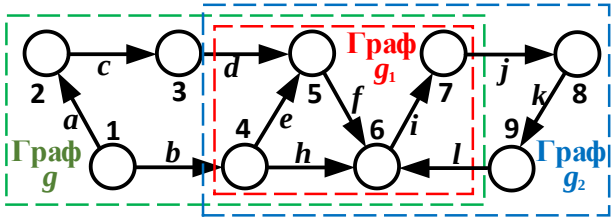
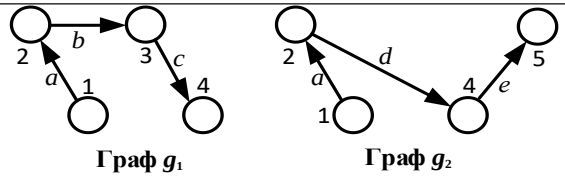
При оценке динамики изменения сетевых инфраструктур теорией графов вводится понятие графа измерений, представляющего собой граф топологии сети, взвешенный множеством измеренных значений сетевых элементов и связей (каналов, соединений).

Для диагностики аномального поведения сети авторами предложен базовый перечень граф-метрик (расстояний между графами) $d(g, g')$, представленный в таблице 11.

Далее представлены леммы [77], описывающие порядок проведения измерений на основе расстояний редактирования графов.

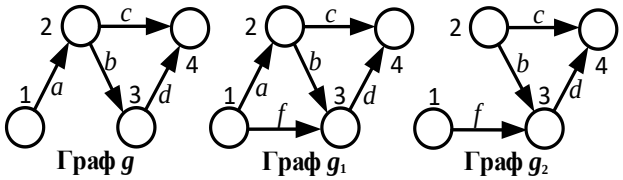
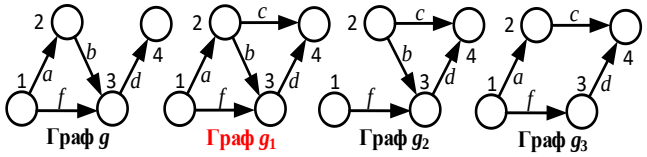
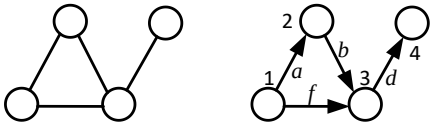
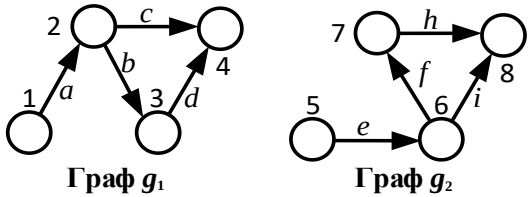
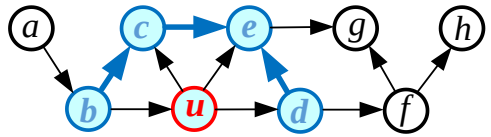
DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

Таблица 11 – Базовые понятия методов на основе расстояния редактирования графов

Определения	Графическое представление графа сети	Математическая запись
Определение 1. Пусть дан граф $g = (V, E, \alpha, \beta)$, где V – множество вершин, E – множество ребер, α и β соответствуют функциям разметки вершин и ребер. Тогда $\alpha: V \to L_V$; $\beta: E \to L_E$, соответствуют множествам *меток узлов* L_V и *меток ребер* L_E.		Размеченный граф: $g = \{\alpha(1, 2, 3, 4, 5, 6, 7); \beta(a, b, c, d, e, f, h, i)\}$.
Определение 2. Пусть даны графы $g = (V, E, \alpha, \beta)$ и $g_1 = (V_1, E_1, \alpha_1, \beta_1)$. g_1 *подграф* g если $V_1 \subseteq V$, $E_1 \subseteq E$, $\alpha(x) = \alpha_1(x)$, $\beta(x, y) = \beta_1(x, y)$ для любых x и y. Обозначим это выражением $g_1 \subseteq g$.		$g = \{\alpha(1, 2, 3, 4, 5, 6, 7); \beta(a, b, c, d, e, f, h, i)\}$. $g_1 = \{\alpha(4, 5, 6, 7); \beta(e, f, h, i)\}$.
Определение 3. Пусть даны графы $g = (V, E, \alpha, \beta)$, $g_1 = (V_1, E_1, \alpha_1, \beta_1)$ и $g_2 = (V_2, E_2, \alpha_2, \beta_2)$. Если $g_1 \subseteq g$ и $g_1 \subseteq g_2$, то g_1 – *общий подграф* g *и* g_2.		$g = \{\alpha(1, 2, 3, 4, 5, 6, 7); \beta(a, b, c, d, e, f, h, i)\}$. $g_1 = \{\alpha(4, 5, 6, 7); \beta(e, f, h, i)\}$. $g_2 = \{\alpha(4, 5, 6, 7, 8, 9); \beta(e, f, h, i, j, k, l)\}$.
Определение 4. Пусть даны $g = (V, E, \alpha, \beta)$, $g_1 = (V_1, E_1, \alpha_1, \beta_1)$ и $g_2 = (V_2, E_2, \alpha_2, \beta_2)$. Если $g_1 \subseteq g$ и $g_1 \subseteq g_2$ и не существует другого общего графа $g' = (V', E', \ldots)$, такого что $V_1 \subset V'$ и $E_1 \subset E'$, то g_1 – *максимальный общий подграф* g и g_2.		(*maximal common subgraph – MCS*) Граф $g_1^{max} = \{\alpha(4,5,6,7); \beta(e,f,h,i)\}$ является максимально общим подграфом графа $g = \{\alpha(1,2,3,4,5,6,7); \beta(a,b,c,d,e,f,h,i)\}$ и графа $g_2 = \{\alpha(4,5,6,7,8,9); \beta(e,f,h,i,j,k,l)\}$.
Определение 5. *Метрика изменения (редактирования) графа*. (*graph edit distance, GED*). Над графом возможно производить следующие виды операций: замена метки узла; замена метки дуги; вставка узла; вставка дуги; удаление узла; удаление дуги.	 Расстояние между графами g_1 и g_2 равно 6: поскольку: удалены узел (3) и ветви (b, c); добавлены узел (5) и ветви (d, e). Следовательно расстояние редактирования $d(g_1, g_2) = 1+2+1+2 = 6$.	Метрики соответствия в сетевых графах: *замена метки узла* → изменение состояния узла; *замена метки дуги* → изменение состояния канала связи; *вставка узла* → восстановление (наращивание) узлов сети; *вставка дуги* → восстановление (добавление) канала связи; *удаление узла* → отказ узла (деградация сети); *удаление дуги* → отказ канала (нарушение связности – деградация).

DOI: 10.24412/2410-9916-2021-4-125-227
URL: https://sccs.intelgr.com/archive/2021-04/07-Allakin.pdf

Таблица 11 – Базовые понятия методов на основе расстояния редактирования графов (продолжение)

Определения	Графическое представление графа сети	Математическая запись
Определение 6. Поставим в соответствие каждой операции e её стоимость $c(e)$. Пусть в течение временинаблюдения за сетью $[t, t+1]$ граф $g = (V, E, \alpha, \beta)$перешел в граф $g_1 = (V_1, E_1, \alpha_1, \beta_1)$. Тогда метрика изменения графа $d(g, g_1)$ будет минимальнасуммарной стоимости операций, переводящих граф g в граф g_1. *Минимальные графы*		$d(g,g') = \min c(s) = \min\left\{\sum_{i=1}^{N} c(e_i)\right\}$. $d(g,g_1) = 1$; $c(e) = 1$. $d(g,g_2) = 2$; $\sum c(e_i) = 2$. $d(g_1,g_2) = 1$; $c(e) = 1$. Минимальные графы g и g_1, g_1 и g_2, поскольку: $d(g,g_1) = \min$, $d(g,g_1) = \min$, а $d(g,g_1) \neq \min$
Определение 7. *Медианой* множества графов $G = \{g_1, \ldots, g_n\}$ называется граф g' такой, что суммарное расстояние от него до каждого графа минимально, т. е. граф g' является центром масс.		$\sum_{i=1}^{N} d(g', g_i) = \min\left\{\sum_{i=1}^{N} d(g', g_i) \mid g \in G\right\}$. Медианный граф множества $G = \{g, g_1, g_2, g_3\}$ есть граф g_1, т. к. $d(g_1,g) = d(g_1,g_2) = d(g_1,g_3) = \min$ и при этом $d(g_1,g_2) = d(g_1,g_3) = d(g_2,g_3) \neq \min$.
Определение 8. Пусть дан граф $g = (V, E, \alpha, \beta)$. *Представление графа в метках* $\rho(g) = (L, C, \lambda)$, где: $L = \{\alpha(x) \mid x \in V\}$, $C = \{\alpha(x), \alpha(y) \mid (x, y) \in E\}$, и $\lambda(\alpha(x), \alpha(y)) = \beta(x, y)$ для всех дуг $(x, y) \in E$.		Размеченный граф: $g = \{\alpha(1, 2, 3, 4); \beta(a, b, d, f)\}$.
Определение 9. Два графа $g = (V, E, \alpha, \beta)$ и $g_1 = (V_1, E_1, \alpha_1, \beta_1)$ *изоморфны* друг другу если существуют взаимооднозначные соответствия между множествами вершин и ребер (имеется возможность их переназначения). Изоморфные графы обладают одними и теми же свойствами и характеристиками.	 Граф g_1 изоморфен графу g_2, поскольку $d(g_1, g_2) = 0$	Графы $g=(V,E,\alpha,\beta)$ и $g_1=(V_1,E_1,\alpha_1,\beta_1)$ изоморфны если: существует биективная функция отображения вершин графа f: $V \rightarrow V_1$; для всех вершин имеет место равенство функций $\alpha(x) = \alpha_1(x)$; для всех ребер $(x,y) \in E$, существует такой набор $(f(x), f(y)) \in E_1$, $\beta(x, y) = \beta_1(f(x), f(y))$ и для всех ребер $(x_1, y_1) \in E_1$, существует такой набор $(f^{-1}(x_1), f^{-1}(y_1)) \in E_1$, $\beta_1(x_1,y_1) = \beta(f^{-1}(x_1), f^{-1}(y_1))$.
Определение 10. *Соседний подграф вершины* в $g_1=(V_1,E_1,\alpha_1,\beta_1)$ это подграф $g_1=(V'_1(u),E'_1(u),\alpha'_1,\beta'_1)$, где $E'_1(u)$ – множество инцидентных дуг между смежными вершинами в $N_1(u)$		Граф соседей вершины ***u*** $g_1=(V'_1(u),E'_1(u),\alpha'_1,\beta'_1)$, $E'_1(u) = E'_1(u)=E_1 \cap [N_1(u) \times N_1(u)]$ – множество инцидентных дуг между смежными вершинами в $N_1(u)$

№4. 2021
ISSN 2410-9916

Лемма 1 [77]: Пусть даны графы $g=(V,E,\alpha,\beta)$, с представлением $\rho(g)$ и $g_1=(V_1,E_1,\alpha_1,\beta_1)$ с представлением $\rho(g_1)$. Граф g изоморфен графу g_1 только и если только $\rho(g) = \rho(g_1)$, т. е. $L_1 = L$, $C_1 = C$, $\lambda_1 = \lambda$.

Лемма 2 [77]: Пусть даны графы $g=(V,E,\alpha,\beta)$, с представлением $\rho(g)$ и $g_1=(V_1,E_1,\alpha_1,\beta_1)$ с представлением $\rho(g_1)$. Граф $g_1 \subseteq g$ только и если только $L_1 \subseteq L$, $C_1 \subseteq C$ и $\lambda_1(i, j) = \lambda(i, j)$ для всех i, j.

Лемма 3 [77]: Пусть даны графы $g=(V,E,\alpha,\beta)$ с представлением $\rho(g) = (L, C, \lambda)$, $g_1=(V_1,E_1,\alpha_1,\beta_1)$ с представлением $\rho(g_1) = (L_1,C_1,\lambda_1)$, и $g_2=(V_2,E_2,\alpha_2,\beta_2)$ с представлением $\rho(g_2) = (L_2,C_2,\lambda_2)$. Пусть $L = L_1 \cap L_2$, $C = \{(i, j)|(i, j) \in C_1 \cap C_2\}$. Тогда граф g – максимальный общий граф графов g_1 и g_2, или $MCS(g_1, g_2)$.

Лемма 4 [77]: Пусть даны графы $g=(V,E,\alpha,\beta)$ с представлением $\rho(g) = (L, C, \lambda)$, $g_1=(V_1,E_1,\alpha_1,\beta_1)$ с представлением $\rho(g_1) = (L_1,C_1,\lambda_1)$, и $g_2=(V_2,E_2,\alpha_2,\beta_2)$ с представлением $\rho(g_2) = (L_2,C_2,\lambda_2)$. Пусть $L = L_1 \cap L_2$, $C = \{(i,j)|(i,j) \in C_1 \cap C_2\}$. Пусть $C_0 = \{(i,j)|(i,j) \in C_1 \cap C_2 \text{ и } \lambda_1(i,j) = \lambda_2(i,j)\}$, $C'_0 = \{(i,j)|(i,j) \in C_1 \cap C_2 \text{ и } \lambda_1(i,j) \neq \lambda_2(i,j)\}$. Тогда:

$$d\ g_1, g_2 = |L_1| + |L_2| - 2|L_1 \cap L_2| + |C_1| + |C_2| - 2|C_0| + |C'_0| \ . \quad (22)$$

Найденное по лемме 4 значение будем далее называть *GED* (Graph Edit Distance – расстояние редактирования графа). Данное выражение следует использовать для оценки состояния сети, оценка ребер которой было уже произведено (например, по классификационной схеме «работоспособное состояние» («норма»), «неработоспособное состояние» («авария»), «предотказное состояние» («предаварийное состояние»).

9.3.3. Взвешенные и невзвешенные расстояния

Помимо приведенного в качестве меры изменения структуры сети может быть использовано следующее выражение [77]:

$$d(g, g') = 1 - \frac{|MCS\ \ g, g'|}{MAX\ \ |g|, |g'|} \ , \quad (23)$$

где $MCS(g, g')$ – максимальный общий граф g_1 и g_2, $|g|$ – число вершин (или ребер) в графе. В качестве более сложных метрик можно использовать и другие [78, 79].

Кроме этого, для графов $g=(V,E,\alpha,\beta)$ и $g_1=(V_1,E_1,\alpha_1,\beta_1)$ можно использовать следующее выражение:

$$d\ g, g' = |V| + |V'| - 2|V \cap V'| + |E| + |E'| - 2|E_0| + |E'| \ . \quad (24)$$

Как следует из вышеизложенного, при равенстве двух графов, расстояние будет минимальным и равным 0. В случае если графы не пересекаются $g \cap g' = \emptyset$, расстояние будет максимальным.

Однако, данные выражения следует использовать для оценки динамики структуры, сети, т. к. они не могут дать оценку изменения взвешенного графа, характеризуемого функциями α, β.

Для оценки взвешенного графа также может быть использовано следующее выражение [80, 81]:

$$d\ g, g' = \frac{|\beta\ u, v\ - \beta'\ u, v\ |}{\max\ \beta\ u, v\ , \beta'\ u, v} \ . \quad (25)$$

Деление полученного выражения на общее число ребер, т. е. на $|E \cup E'|$ позволит оценить вариацию вектора характеристик ребер для графа в целом. В указанной формуле, в случае отсутствия того или иного ребра, вес последнего считается равным 0.

9.3.4. Анализ редактирования на основе спектра графов сети

Пусть задан граф $g=(V,E,\alpha,\beta)$ с матрицей смежности вершин A_g. Спектром графа $\sigma(g)$ назовем последовательность собственных чисел матрицы A_g $\{\lambda_1,\lambda_2,\ldots,\lambda_n\}$.

В настоящее время известна также другая методика исследования свойств (неориентированного) графа на основе собственных чисел матрицы Кирхгофа (Лапласиан графа) [82]: $L_g = D_g - A_g$, где D_g – матрица степеней определяется следующим образом:

$$D_g = \mathrm{diag}\left\{\sum_{v\in V} \beta\ u,v\ \mid u \in V_g\right\}.$$

В случае невзвешенного графа, элементами матрицы D_g будут степени вершин.

В случае ориентированного графа матрица Кирхгофа определяется следующим выражением: $L_g = D_g - A_g + A_g^T$.

На основе полученных собственных значений матрицы смежности вершин графа или матрицы Кирхгофа вычисляется расстояние между графами (*GED*) [77]:

$$d\ g,g' = \sqrt{\frac{\sum_{i=1}^{k} \lambda_i - \mu_i\ ^2}{\min\left\{\sum_{i=1}^{k}\lambda_i^{\,2}, \sum_{i=1}^{k}\mu_i^{\,2}\right\}}}\ . \qquad (26)$$

Для спектров графов $\sigma\ A_g = \lambda_1,\lambda_2,...,\lambda_n$, $\sigma\ A_{g'} = \mu_1,\mu_2,...,\mu_n$ k – эмпирически выбранный предел суммирования. В приложениях распознавания образов и обработки изображений экспериментально установлено оптимальное значение k = 20.

9.3.5. Сетевые измерения на основе структуры графа

Для вершин $u, v \in V_g$ рассмотрим следующее множества путей графа:

$P_k^g\ u,v$ – путей длины k, соединяющих вершины u и v;

P_k^g – совокупность путей длины k в графе;

$P_k^g\ u,v = \bigcup_{k>2} P_k^g\ u,v$ – множество путей длины большей 2 соединяющих вершины u и v;

$P^g = \bigcup_{k\geq 2} P_k^g$ – совокупность всех путей.

Передача данных в сети осуществляется посредством маршрутов, поэтому удаление вершины приводит к отказу маршрутов, содержащих данную вершину в качестве промежуточной. Исходя из этих соображений в качестве чувствительной метрики состояния сети можно использовать рассмотренное ранее расстояние редактирования *GED*, основанное на числе путей, содержащих заданную вершину(ы).

Для выделенного (непустого) подмножества ребер $\hat{E} \subseteq E$, сформируем новый граф $g\ \hat{E} = V', E', \alpha, \beta$, таким образом, что в исходном графе остаются только те дуги, которые содержатся в маршрутах, содержащих дуги из $\hat{E} \subseteq E$. Более формально, граф $g\ \hat{E}$ формируется следующим образом:

$V' = V$.

Ребро $e \in E'$ тогда и только тогда, когда $\exists p \in P_k^g : e \in p$ и $\exists e_1 \in \hat{E}, e_1 \in p$.

$\alpha' = \alpha$.

Веса ребер в G_g равны числу маршрутов в P^g, содержащих данное ребро в качестве компонента (и, по крайней мере, одно ребро из предопределенного набора $\hat{E} \subseteq E$).

Атрибуты весов в созданном описанным способом графе $g\ \hat{E}$ отражают степень важности ребер в процессах передачи данных через сеть, и поэтому определяют степень влияния на связность узлов.

Сравнение двух созданных на основе $g_1 = (V_1, E_1, \alpha_1, \beta_1)$ и $g_2 = (V_2, E_2, \alpha_2, \beta_2)$ графов, может быть осуществлено по формуле (24). В качестве $\hat{E}$ выбирается E_1 и E_2. Также можно использовать множество ребер $mcs(g_1, g_2)$. Общей рекомендаций при создании $\hat{E}$ является включение наиболее значимых связей сети.

Вариантом описанной методики является исследование 2-компонентной связности графа. В результате смежные вершины в полученном графе соответствуют вершинам исходного графа, соединенных через общего соседа. Как результат, полученная структура более чувствительна к изменениям в топологии (включение/исключением вершин, ребер), нежели исходная структура. Однако в данном случае, граф остается невзвешенным. Сравнение полученных структур может быть произведено по формулам (23) и (24).

9.3.6. Идентификация областей изменения

Симметричная разность графов

При анализе динамики сети важным является не только установление факта изменения, приводящего к ошибкам, но и выявление компонент графа сети, приводящих к возникновению событий.

Расстояние между двумя графами $g_1 = (V_1, E_1, \alpha_1, \beta_1)$ и $g_2 = (V_2, E_2, \alpha_2, \beta_2)$ может быть охарактеризовано при помощи матрицы изменений $C = [C_{uv}]$, элементы которой соответствуют удаленным из g_1 или добавленным в g_2. Строки и столбцы матрицы C соответствуют множеству $V_1 \cup V_2$. В случае удаления или добавления ребра (u,v) соответствующий элемент матрицы будет равен 1, в случае если соответствующее ребро присутствует в обоих графах, соответ-

ствующий элемент будет равен 0. Данная матрица описывает граф, называемый *симметричной разницей графов* и обозначается $g_1 \Delta g_2$.

Сумма элементов по строкам (или столбцам) матрицы C дает вектор изменений относительно вершин объединенного множества $V_1 \cup V_2$. Ранжирование с последующим выделением n максимальных компонент позволяет локализовать области изменений.

Указанный подход может быть распространен на взвешенные графы, при этом компоненты симметричной разности вычисляются по формуле:

$$C_{u,v} = \frac{\left|\beta\ u,v\ - \beta'\ u,v\ \right|}{\max\ \beta\ u,v\ ,\beta'\ u,v\ }, \tag{27}$$

где $u,v\ \in E_1 \cup E_2$.

Аналогично, для анализа динамики может быть использована группа симметричных разностей высшего порядка:

$$g_i \Delta^2 g_{i+2} = g_i \Delta g_{i+1}\ \Delta\ g_{i+1} \Delta g_{i+2}\ ,$$

$$g_i \Delta^3 g_{i+4} = g_i \Delta^2 g_{i+2}\ \Delta\ g_{i+2} \Delta^2 g_{i+4}\ ,$$

...

Анализ на основе графа соседей вершин

Альтернативой симметричной разности является подход на основе измерения расстояния между соответствующими (последовательными во времени) графами соседей вершины (определение 10 в таблице 11). Данная техника позволяет получить вектор расстояний между графами из g_1 и g_2. Каждая координата вектора соответствует расстоянию между графами соседей с «точки зрения» отдельной вершины и смежных с нею вершин, что и позволяет *выявить области изменений.*

Последовательные измерения по времени состояния сети по описывающим их графам могут быть сравнены, используя описанный выше подход, где в качестве измерения расстояния между графами применить формулы (22-25). Граф соседей вершины, присутствующей только в одном графе, сравнивается с пустым графом. Результатом операции является вектор расстояний графов соседей вершин: $d = \left[d\ \ g_1'\ u\ , g_2'\ u\ \right]$.

Соседний подграф вершин описывает связи с вершинами, связанными 1 дугой. Для целей анализа целесообразно также рассмотреть 2-соседний граф, описывающий 1 и 2-компонентную связность, т. е. включающий 1 и 2 достижимые вершины, вместе с связывающими их ребрами, рис. 26.

Исследование чувствительности предложенных метрик на основе расстояния редактирования графа, метрик на основе максимального общего подграфа и метрик на основе спектра графа были исследованы в [77] на базе данных, полученных при эксплуатации корпоративной сети передачи данных с помощью инструментов NetFlow. В сети передачи данных использовались статические IP-адреса, которые соответствовали меткам. Графы сети были построены с интервалом в один день. Результатом явился временной ряд из 100 графиков. Ре-

зультаты показывают одинаковую чувствительность к структурным изменениям ИТКС [75]. При этом на 20-й, 69-й и 90-й день наблюдаются аномальные перестройки графа, рис.27-30.

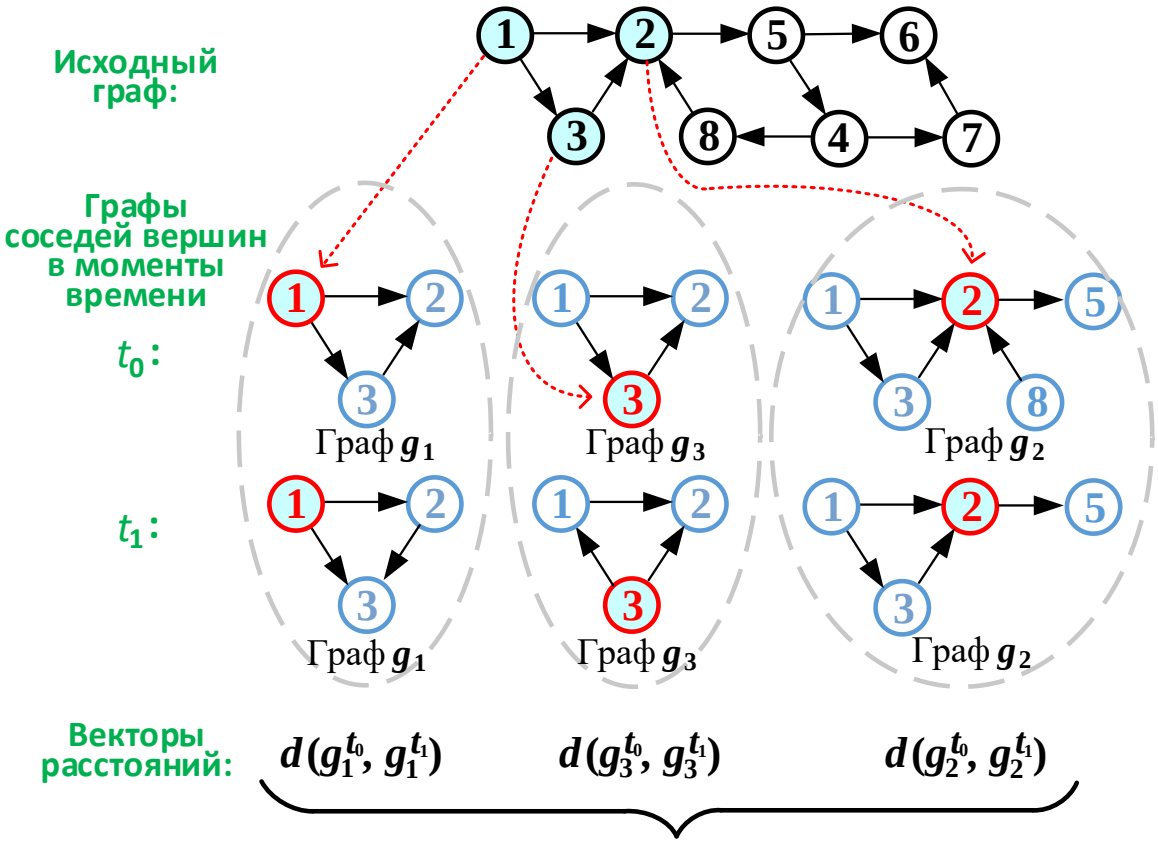


Рис. 26. Сетевые измерения на основе графов соседей

Спектральная теория графов на сегодня активно применяется в химии, когда молекулы химического соединения представляются в виде графов, в которых атомы являются вершинами, а валентные соединения атомов между собой – ребрами. Тогда применяя собственные числа матрицы Лапласа, определяются (прогнозируются) химические свойства соединений.

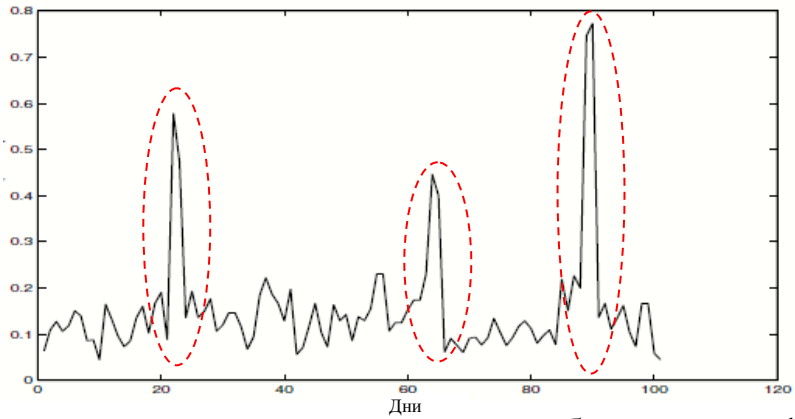
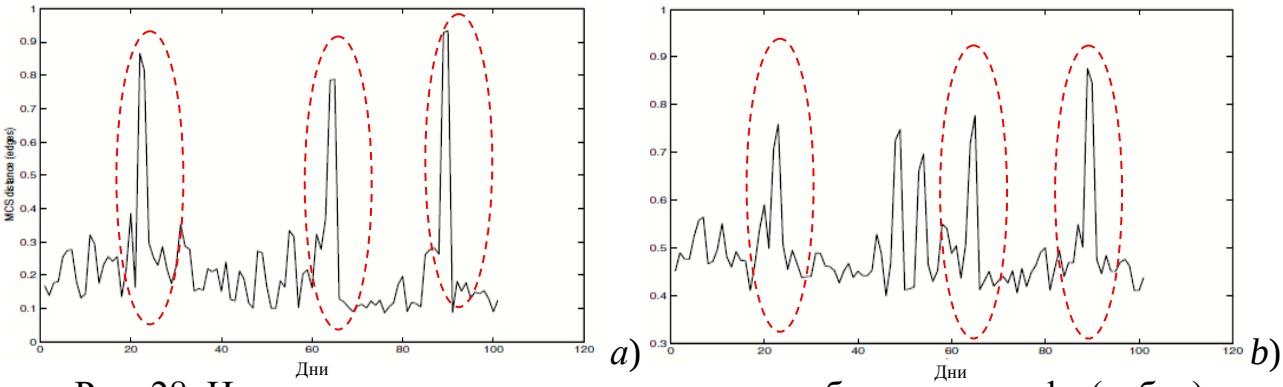


Рис. 27. Измерение на основе максимального общего подграфа(вершины) (MCS)



a) *b*)

Рис. 28. Измерение на основе максимального общего подграфа (ребра):
a) Метрика MCS (ребра) без учета весов. Расстояние MCS (края),
b) Метрика MCS (ребра) с учетом весов. Общее расстояние между кромками-весов

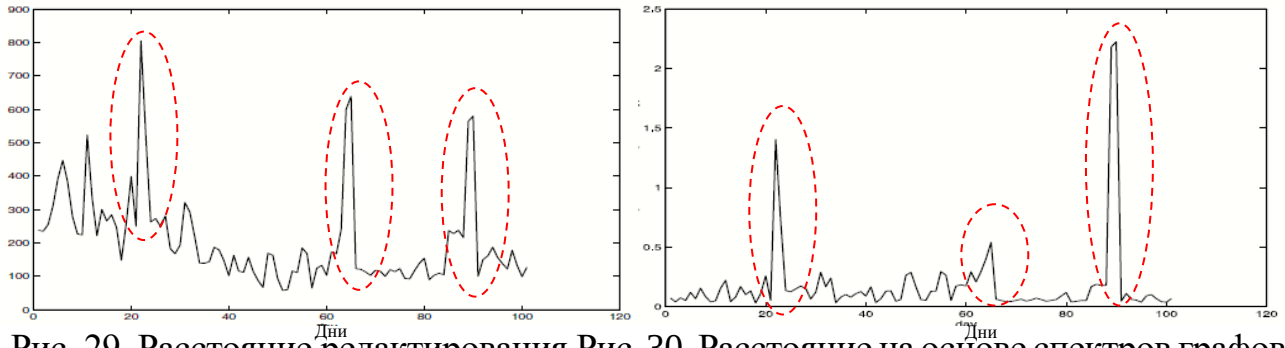


Рис. 29. Расстояние редактирования Рис. 30. Расстояние на основе спектров графов

9.3.7. Средние графы

Согласно определению, медианным граф $\bar{g}$ последовательности $G = \{g_1, g_2,\ldots,g_n\}$ называется такой граф, суммарное *GED* которого до каждого члена последовательности минимально: $\bar{g} = \arg\min_{g \in U} \sum_{i=1}^{n} d\ g, g_i$.

Рассмотрим *GED*, обобщающее формулу (23) [77]. Будем считать, что операция замены метки ребра с весом $\beta_1(e)$ на метку с весом $\beta_2(e)$ будет иметь стоимость $|\beta_1(e) - \beta_1(e)|$. В случае добавления или же удаления ребра из графа, стоимость операции будет равна весу ребра, т. е. $|\beta_1(e) - 0|$.

$$d_2\ g_1, g_2 = c \cdot \left[\left|V_1\right| + \left|V_2\right| - 2\left|V_1 \cap V_2\right|\right] + \\ + \sum_{e \in E_1 \cap E_2} \left|\beta_1\ e - \beta_2\ e\right| + \sum_{e \in E_1 \setminus E_1 \cap E_2} \beta_1\ e + \sum_{e \in E_2 \setminus E_1 \cap E_2} \beta_2\ e \ . \quad (28)$$

Константа c позволяет учитывать величину влияния операций вставки/удаления узлов по отношению к операции над ребрами графа.

Рассмотрим объединенный граф $g = (V, E, \alpha, \beta)$ последовательности $G = \{g_1, g_2,\ldots,g_n\}$, где $V = \bigcup_{i=1}^{n} V_i$, $E = \bigcup_{i=1}^{n} E_i$ и обозначим через $\gamma(u_i)$ число повторений вершины u_i в последовательности графов.

Определим граф $g = (V, E, \alpha, \hat{\beta})$ следующим образом:

$$\begin{aligned} \hat{V} &= \{u \mid u \in V \text{ и } \gamma(u) > n/2\}, \\ \hat{E} &= \{(u,v) \mid u,v \in \hat{V}\}, \\ \hat{\beta}(u,v) &= \text{med}\{\beta_i(u,v) \mid i = 1...n\}. \end{aligned} \tag{29}$$

Согласно теореме, доказанной в [77], данный граф является медианным (средним) по *GED*, вычисляемому по формуле (28). Он не является уникальным, т. к. операция вставки-замены узла позволяет получить семейство средних графов.

9.3.8. Применение средних графов для выявления аномальных состояний сети

Усреднение последовательности графов позволяет исключить влияние случайных флуктуаций, что подобно действию суммирующего фильтра при размытии сигнала. Поэтому данный метод, в отличие от выше рассмотренных более предпочтителен для выявления долговременных тенденций в поведении сети.

Сравнение среднего графа с последующим одиночным (msa)

В данном процессе производится вычисление среднего графа по «скользящему окну» длиной *L*, рис. 31.

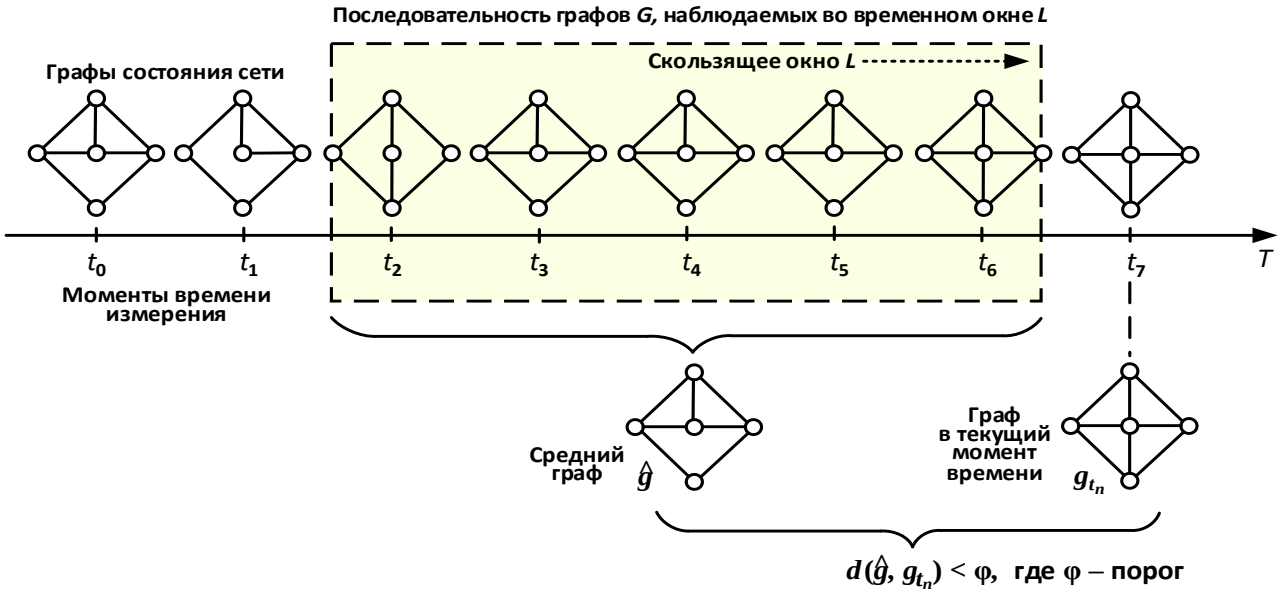


Рис. 31. Процедура *msa* – сравнение (измерение) среднего графа с последующим одиночным

Пусть $\hat{g}$ – средний граф последовательности $G = \{g_{n-L+1}, g_{n-L+2}, \ldots, g_n\}$. Тогда расстояние, $d_2(\hat{g}, g_{n+1})$, в сравнении с предопределенным порогом может быть использовано для выявления *аномальных* (*скачкообразных*) *изменений*

в поведении сети. В качестве порога можно использовать среднее изменение *GED* сети по скользящему окну:

$$\varphi = \frac{1}{L}\sum_{i=n-L}^{n} d_2\ \hat{g}_n, g_i\ .$$

Событие «аномальное поведение сети» генерируется при условии:

$$d_2\ \hat{g}_n, g_{n+1}\ \geq \alpha\cdot\varphi\ .$$

Как было указано, средний граф не является уникальным, в связи с чем, если было получено семейство средних графов $\left(\hat{g}_{n_1}, \hat{g}_{n_2}...\hat{g}_{n_m}\right)$, можно вычислить набор пороговых значений (φ_1, φ_2,…, φ_m). Решение о состоянии сети можно определить из следующего условия:

$$d_2\ \hat{g}_{n_1}, g_{n+1}\ \geq \alpha\cdot\varphi_1 \wedge d_2\ \hat{g}_{n_2}, g_{n+1}\ \geq \alpha\cdot\varphi_2 \wedge ... \wedge d_2\ \hat{g}_{n_m}, g_{n+1}\ \geq \alpha\cdot\varphi_m\ .$$

Сравнение среднего графа с последующим средним (mma)

В данной схеме (рис. 32) в последовательных скользящих окнах L_1 $G_1 = g_{n-L+1},...,g_n$ и L_2 $G_2 = g_{n-L+1},...,g_{n+L+2}$ вычисляются средние графы $\hat{g}_n$ и $\hat{g}_{n+1}$. В качестве правила принятия решения о состоянии сети используется следующее уравнение:

$$d_2\ \hat{g}_n, \hat{g}_{n+1}\ \geq \alpha\cdot\left[\frac{L_1\varphi_1 + L_2\varphi_2}{L_1 + L_2}\right].$$

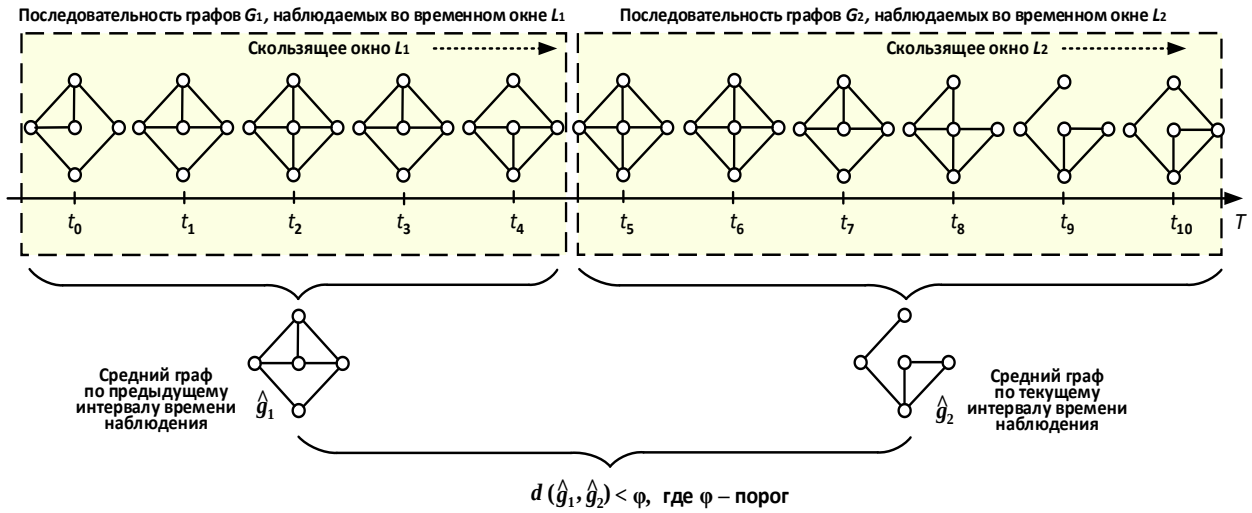


Рис. 32. Процедура *mma* – сравнение (измерение) среднего графа с последующим средним

Сравнение среднего графа с удаленным одиночным (msd)

В случае, если имеет место *постепенное изменение* состояния сети, целесообразно сравнивать средний граф $\hat{g}_n$ не с последующим g_{n+1}, а с отстоящим на *l* измерений, где *l* выбирается эвристически, рис. 33.

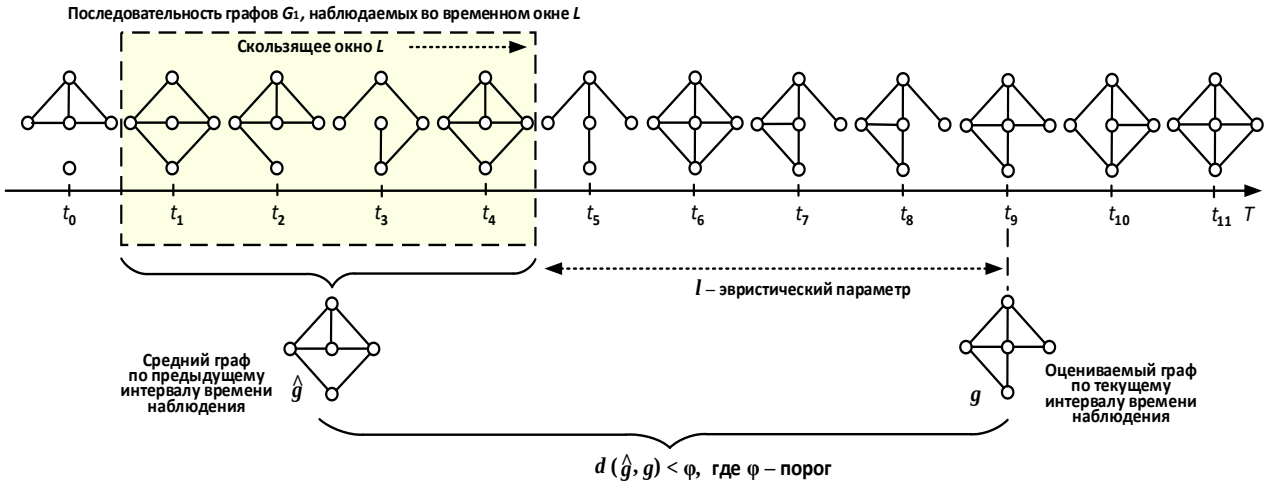


Рис. 33. Процедура *msd* – сравнение (измерение) среднего графа с последующим одиночным

Сравнение среднего графа с удаленным средним (mmd)

Данный метод представляет собой комбинацию предыдущего случая и сравнения последовательных средних. Как описано выше, рассмотрим средний граф $\hat{g}_1$ по множеству $G_1=\{g_{n-L1+1},\ldots,g_n\}$ и $\hat{g}_2$ по множеству $G_2=\{g_{n+l+1},\ldots,g_{n+l+L}\}$. Сравнение удаленных друг от друга граф-измерений позволяет оценить абсолютную величину «постепенного» изменения состояния сети, рис. 34.

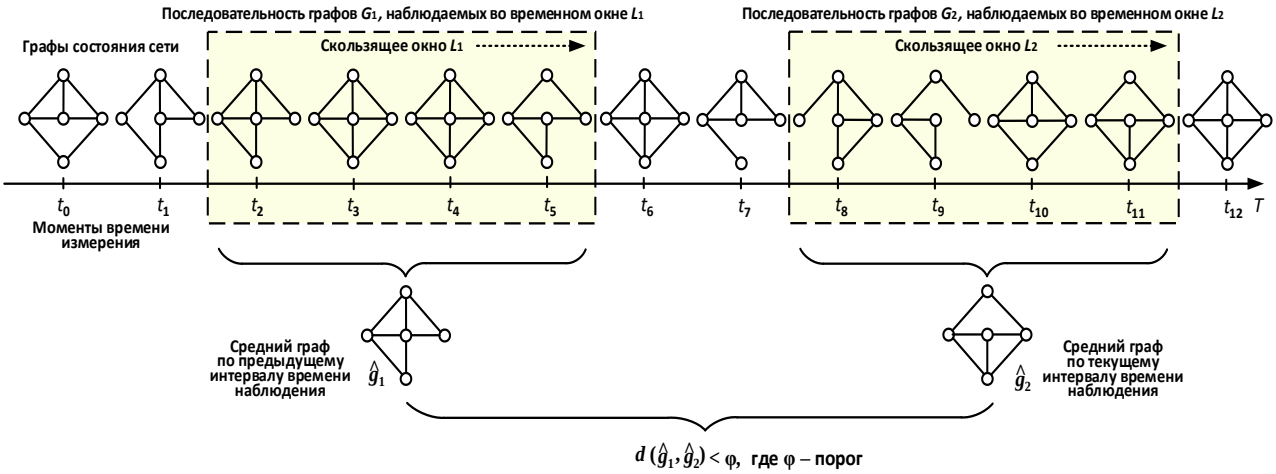


Рис. 34. Процедура *mmd* – сравнение (измерение) среднего графа с удаленным средним

Рассмотренные выше процедуры (*msa*, *mma*, *msd* и *mmd*) применения средних графов для выявления аномальных состояний сети заимствованы из теории графов, активно применяемой на сегодня в интеллектуальных системах распознавания образов (распознавание лиц, жестов рук, отпечатков пальцев, радужной оболочки глаз и пр.).

В таблице 12, приведены сведения по областям практического применения методов на основе расстояний редактирования графа.

Таблица 12 – Примечание по реализации базового набора характеристик сети

Наименование характеристик	Формулы расчета	Примечания по реализации	Примечание по отображению
Общая динамика сети	Базовое расстояние (формула 24)	Вычисление производят на основе пары графов в формате разреженных матриц	В виде графика функции
Общая динамика сети	Расстояние на основе спектра графа (формула 28)	Вычисление производят на основе пары графов в формате разреженных матриц	В виде графика функции
Динамика структуры сети	Расстояние по структуре графов (формула 26)	Вычисление производят на основе пары графов в формате разреженных матриц	В виде графика функции
Динамика маршрутов передачи данных	Суммарное расстояние редактирования (расстояние Левенштейна)	Вычисление производят на основе пары графов в формате разреженных ма-триц и файлов маршрута	В виде линейного графика
Приоритеты связей	Веса дуг графа, полученный при расчете динамики маршрутов	Вычисление производят на основе пары графов и файлов маршрута	В виде столбчатых диаграмм. При отображении осуществляют ранжирование. На графике виден прирост /убыль значимости связи
Локализация изменений в сети	Вычисление вектора изменений на основе симметричной разности и на основе подграфов соседей вершин	Вычисление производится на основе пары графов	В виде столбчатых диаграмм. При отображении осуществляют ранжирование. На графике виден прирост/убыль значимости связи

При этом для идентификации состояния сетевой инфраструктуры в результате сбора измерительной информации в каждый из моментов времени наблюдения (мониторинга) t, t+1, t+2, и т. д. строятся графы сети и производятся измерения расстояний между графами соседей. Метрикам изменения (редактирования) графов в динамике (во времени) можно поставить в соответствие идентификацию следующих состояний элементов претерпевающей изменения на этапе ЖЦ динамической ИТКС:

– замена метки узла → изменение состояния узла;
– замена метки дуги → изменение состояния канала связи;
– вставка узла → восстановление (наращивание) узлов сети;
– вставка дуги → восстановление (добавление) канала связи;
– удаление узла → отказ узла (деградация сети);
– удаление дуги → отказ канала (нарушение связности – деградация сети).

Определяются метрики изменения двух соседних графов g и g_1 анализируемой сети графовым расстоянием $d(g, g_1)$. При этом на последовательности нескольких графов $G=\{g_1, g_2, \ldots, g_n\}$, наблюдаемых в скользящем временном окне подсистемы сетевого мониторинга, определяется минимальный граф (с минимальной суммарной стоимости операций, переводящих граф g в граф g_1), являющийся медианным или средним графом. По изменению графа соседей верши-

ны в различные моменты времени формируется вектор расстояний между графами соседей, которые сравниваются с пороговым значением. В случае превышения порога графового состояния на очередном временном интервале наблюдения идентифицируется изменение состояния сети (переход сети из одного класса состояния к другому), например деградация или восстановление сети (предотказное состояние или авария) и т. д.

Из перечисленных методов теории графов для анализа сетевых инфраструктур наиболее приемлемы методы на основе расстояния редактирования графов, поскольку они позволяют осуществлять оценку общего состояния сети учитывая техническое состояние, как отдельных сетевых устройств (вершин графа), соединений (ребер графа), а также путей передачи данных (ПД) (маршрутов ПД). В то же время, в архитектуру сети под эти методы необходимо включение компонента интеллектуальной обработки, рис. 35.

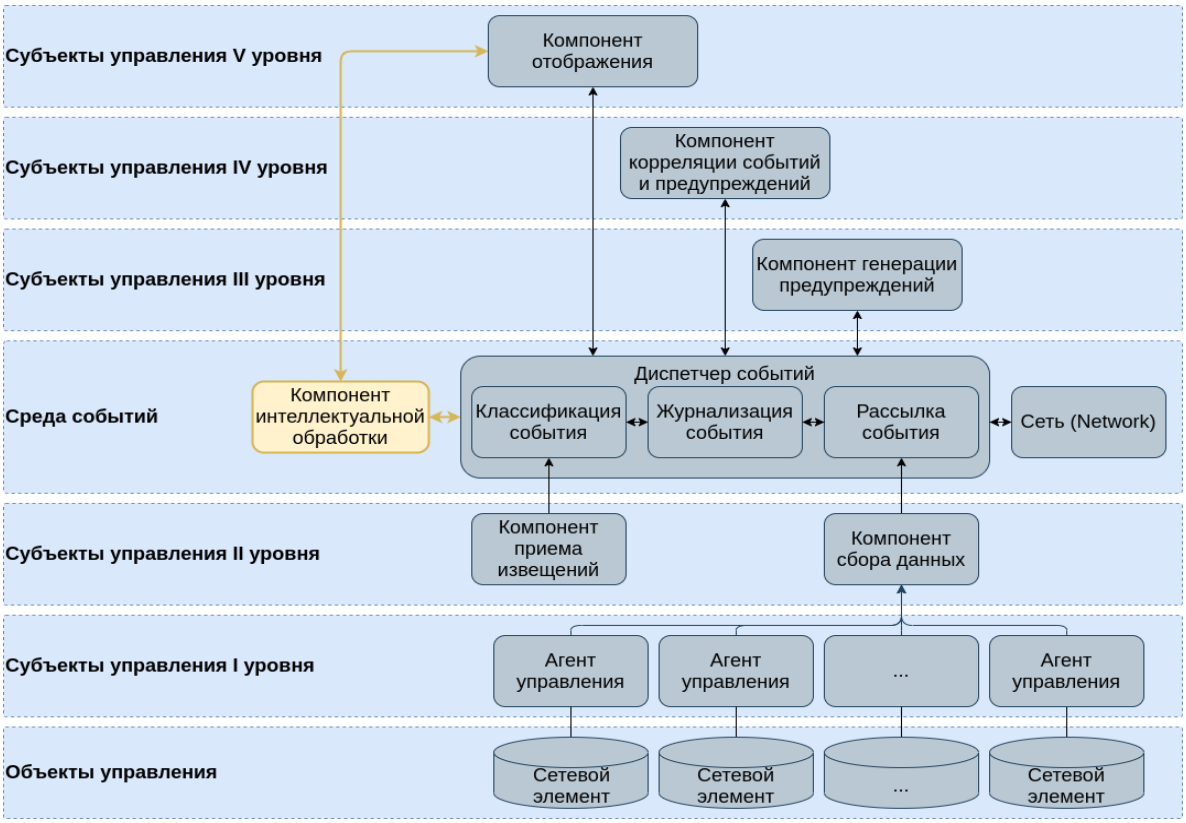


Рис. 35. Обобщенная архитектура перспективной системы мониторинга

10. Алгоритм определения состояния сети на основе измерения графового расстояния и метода *k*-средних

Процедура мониторинга современных сетевых инфраструктур должна осуществляться в режиме реального времени. При этом если в момент времени t состояние наблюдаемой сети принять за исходное состояние (первое множество вершин и ребер на сетевом графе g), то в промежуток времени $t + 1$ в силу внутренних (изменение режимов работы, величины обрабатываемого трафика и пр.), а также внешних (ошибки обслуживающего персонала, дестабилизирующие воздействия и пр.) на динамической структуре будет наблюдаться совершенно другое состояние (второе множество вершин и ребер сетевого графа g_1),

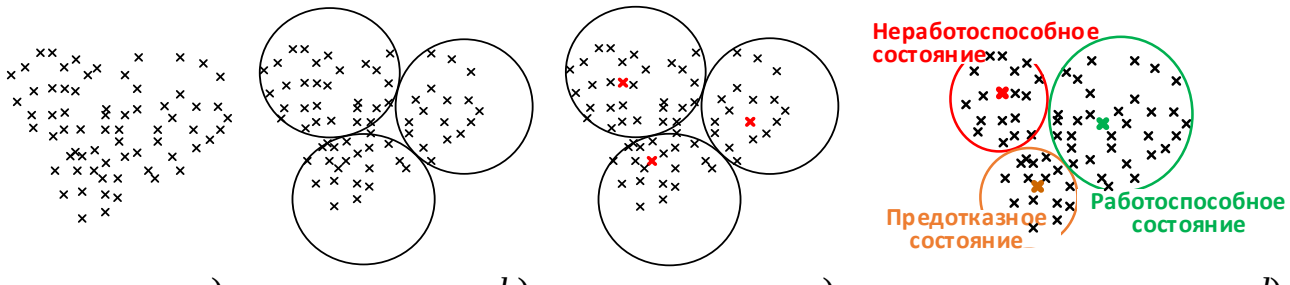
в момент времени $t + 2$ может наблюдаться третье состояние, описываемое сетевым графом g_2, или сеть может вернуться в исходное состояние, описываемое сетевым графом g и т. д. Каждое из этих состояний характеризуется расстоянием между графами $d(g, g_1)$, $d(g, g_2)$ и т. д. Если исходное состояние сети, описываемое графом g принять за эталонное и определить порог на изменение расстояния между ним и новыми графами, образующимися в моменты времени $t + 1$, $t + 2$ и т. д., как и порог на суммарное расстояние от него до каждого образованного графа, то в случае превышения величины порога будем считать, что сеть перешла в другое состояние.

Другими словами, нормальное состояние ИТКС характеризуется допустимыми изменениями топологии сети, что описывается некоторым множеством графов, также, как и другие виды состояний ИТКС определяется также некоторым множеством графов. Данные множества образуют кластеры, в которых средний граф будет являться центром кластера (центром масс).

С учетом вышеизложенного, а также на основании понятия среднего графа (Определение 7 таблицы 11) для идентификации видов состояния ИТКС можно применить алгоритм *k*-средних. При этом, если в ходе обработки наблюдаемых временных рядов параметров метрик, получаемых от сетевых устройств, используется *EM*-алгоритм (рис. 21), то для определения состояния всей сети в целом в работе наиболее подходит при анализе графового расстояния алгоритм *k*-средних (как невероятностный аналог *EM*-алгоритма). Рассмотрим его подробнее.

Процедура алгоритма *k*-средних при определении состояния сети имеет следующие этапы:

На начальном этапе такой подход предполагает, что в качестве исходных данных для идентификации нормального и аномальных состояний сети используются облака данных как неупорядоченные наборы данных, не привязанные к какой-либо из шкал измерений. В отличие от процедуры *TDA*, описанной выше и применяемой для анализа временных рядов метрик сетевых элементов, в предлагаемом алгоритме облако данных представляют в виде множества точек в заданном топологическом пространстве метрик графов, описывающих состояния ИТКС. А поскольку в данном алгоритме исходные данные представлены сетевыми графами, то граф сети преобразуется без потери информации в облако точек, где каждому графу (характеризуемому графовым расстоянием от базового (исходного, спроектированного) графа) ставится в соответствие точка в соответствующем облаке данных, рис. 36 *a*).



a) *b*) *c*) *d*)

Рис. 36. Процедура алгоритма *k*-средних при определении состояния ИТКС ОП

На первом этапе определяется количество кластеров состояний сети. Одной из особенностей алгоритма *k*-средних является заранее определяемое число кластеров. Для мониторинга сетевых инфраструктур, как правило, в конечной интерпретации оператора подсистемы мониторинга таких состояний всего два «работоспособное состояние» («норма») – сеть выполняет свои функции и «неработоспособное состояние» («авария», или блокировка сети). С целью недопущения внезапного перехода сети в аварийное состояние, также особый интерес представляет «предотказное состояние» [7], характеризуемое повышенным риском отказа объекта контроля, возникающего как в результате внутренних процессов и причин, так и внешних воздействий на сеть в процессе ее функционирования. В соответствии с международной классификацией «предотказное состояние» соотносится с «критическому» [12]. В связи с изложенным, на первом этапе произвольно определим на облаке точек три кластера, которые в последующем, после завершения схождения алгоритма *k*-средних, будут соответствовать основным состояниям ИТКС, рис. 36 *b*).

На втором этапе алгоритма выбираются центры масс (центроиды), рис. 36 *c*). Процедура осуществляется по указанному в таблице 11 определению 7 – медианного графа, такого, от которого суммарное расстояние до каждого графа (точек в соответствующем кластере) минимально, т. е. граф, являющийся центром масс в заданном кластере, соответствующем виду технического состояния [7, 12].

На третьем этапе, после анализа графового расстояния и определения медианных графов, соответствующих тому или иному состоянию сети, определяется расстояние до центров масс от каждого из наблюдаемых графов, рис. 36 *d*). Если окажется, что рассматриваемый граф ближе к медианному графу (тяготеет к нему), описывающему первое (нормальное) состояние сети – «1», следовательно состояние данного графа имеет такое же состояние, как и граф с центром «1». Если рассматриваемый граф ближе к медианному графу, описывающего состояние «2», то состояние этого графа имеет такое же состояние, как и граф с центром «2», и т. д. Так на рис. 36 *d*) кластеры, описывающие работоспособное, предотказное и неработоспособное технические состояния выделены цветом.

Как уже отмечалось ранее, в динамической системе, к которой относят и распределенные ИТКС, состояние сети постоянно изменяется. Например, выход из строя узла сети (вершины графа) или канала связи (ребра графа) влечет за собой перемаршрутизацию, направленную на восстановление функционального состояния сети. Поэтому с течением времени сетевой граф будет претерпевать изменения, а, следовательно, на каждом временном интервале мониторинга сети необходима итерация:

– по определению новых кластеров ее состояния в следующий момент времени $t + 1$;
– назначению центров масс (медианных графов), соответствующих видам состояния сети;

– определению расстояния наблюдаемого графа до центров масс медианных графов;
– сравнение вычисленных расстояний и по их минимуму – идентификация вида состояния сети.

Таким образом, итерационная процедура повторяется до момента времени, когда рассматриваемый граф не окажется к центру кластера «2», графа, имеющему «предотказное состояние», или к центру кластера «3», графа, имеющего состояние «авария».

На завершающем этапе компонент интеллектуальной обработки (рис. 35) транслирует на компонент отображения сигнал о виде состояния ИТКС в интересах оператора СППР или АСУС.

Таким образом, рассмотренная процедура определения состояния сети на основе измерения графового расстояния и алгоритма *k*-средних является невероятностной версией *EM*-алгоритма, рассмотренного выше в ходе анализа временных рядов наблюдаемых параметров сетевых устройств, и позволяет производить анализ состояния ИТКС в целом.

Заключение

В работе представлен обзор действующих технологий и систем сетевого мониторинга ИТКС ОП. Дана характеристика таким из них как SCOM, Zabbix, Nagios, Cacti, OSS, Amazon CloudWatch, и др. Их обзор показал, что в межведомственных распределенных ИТКС вычислительные мощности на границах сети растут, а облачные вычисления, традиционно обеспечиваемые предоставлением инфраструктурных услуг в крупных ЦОД, перемещаются на границу сети. Причем рост доступности периферийных инфраструктур также подталкивает приложения, которые обычно работают в удаленных ЦОДах, к работе на распределенных периферийных устройствах. В этих условиях значительно меняются общие подходы и методы построения перспективных подсистем мониторинга сети.

В работе определены функции подсистемы сетевого мониторинга ИТКС и сервера мониторинга, как ключевого ее элемента. Предложен вариант структуры сервера мониторинга ИТКС и зависимых подсистем. Рассмотрены назначаемые объекты мониторинга, а также перечень собираемых с них метрических данных с точки зрения функциональной производительности ИТКС. Сформулированы общие требования к перспективным системам сетевого мониторинга, а также общие принципы организации и функционирования подсистем мониторинга ИТКС – для повышения устойчивости и надежности объекта контроля ключевым архитектурным принципом проектирования современных подсистем мониторинга распределенных гетерогенных ИТКС определен принцип *распределенности* и *децентрализации*.

На основе проведенного анализа научно-методического аппарата оценки временных рядов наблюдаемых метрик предложен подход к формированию методики прогнозирования аномальных ситуаций по результатам мониторинга функционального состояния сетевых элементов ИТКС ОП. При этом превентивная идентификация аномального состояния сетевого элемента осуществляется путем выявления «запрещенных» кодовых комбинаций при наблюдении временных ря-

дов, обработанных заимствованными из биоинформатики методами символической динамики, используемыми ранее в процессе анализа сложных нуклеотидных геномных последовательностей, а также введение особого режима мониторинга, когда при идентификации предотказного ТС скважность опроса сервером мониторинга сетевого элемента значительно увеличивается с целью своевременного принятия превентивных управляющих воздействий на сетевую инфраструктуру для недопущения пропуска отказа сетевого элемента или наступления аварии. В основу предложенного алгоритма заложен метод символического представления временных рядов, на базе которого дана оценка энтропии кодовых слов, описывающих временной ряд наблюдаемой метрики функционирующего сетевого элемента и разработан алгоритм методики идентификации аномальной ситуации на временном ряду его параметров, состоящий из четырех этапов: предварительного этапа, этапа кодирования временных рядов, этапа идентификации вида технического состояния сетевого элемента и завершающего этапа. Данный алгоритм позволит в последующем сформировать порядок функционирования сервера мониторинга для идентификации аномалий в работе ИТКС ОП.

Также в работе представлен обзор групп методов, учитывающих взаимное влияние сетевых элементов в динамике изменения состояния сети на основе методов сетевой томографии, Приведены примеры дискретной (булевской) томографии (где каждое соединение предполагается в двух состояниях – «работает» или «не работает»), а также непрерывной томографии, предполагающей что соединение характеризуется распределением вероятностей. В этом случае путь (последовательность соединений) характеризуется смешанным распределением вероятностей, и задача реконструкции решается *EM*-алгоритмом.

На основе рассмотренных процедур применения средних графов (*msa*, *mma*, *msd* и *mmd*) для выявления аномальных состояний на сети по анализу расстояния между графами в работе применен алгоритм *k*-средних, который в отличие от использования *EM*-алгоритма (для наблюдения за временными рядами параметров метрик, получаемых от сетевых устройств), является невероятностным методом.

Литература

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

2. ITU-T: General principles and general reference model for Next Generation Networks. Recommendation Y.2011 – Geneva, 2004. – URL: https://www.itu.int/rec/T-REC-Y.2011-200410-I/en (дата обращения: 30.07.2021).

3. 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. – URL: https//doi:10.23919/INM.2017.7987291 (дата обращения 03.07.2021).

4. Будко П. А. Управление ресурсами информационно-телекоммуникационных систем. Методы оптимизации. Монография. – СПб.: ВАС, 2012. – 512 с.

5. 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. doi: 10.24411/2409-5419-2018-10293.

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

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

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

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

10. Легков К. Е., Бабошин В. А., Нестеренко О. Е. Модели и методы управления современными мультисервисными сетями связи // Техника средств связи. 2018. № 2 (142). С. 181-182.

11. Легков К. Е. Процедуры и временные характеристики оперативного управления трафиком в транспортной сети специального назначения пакетной коммутации // T-Comm: Телекоммуникации и транспорт. 2012. Т. 6. С. 42-46.

12. 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 03.07.2021).

13. Новый подход к обучению сетевым технологиям. Изучение сетевого оборудования Cisco, протоколов и механизмов посредством построения крупной корпоративной сети. – URL: https://www.darkmaycal-it.ru/cisco (дата обращения 03.07.2021).

14. 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.

15. TechNet Magazine: System Center Operations Manager 2012: Простота расширения возможностей мониторинга. – URL: http://technet.microsoft.com (дата обращения 03.07.2021).

16. Vacche A. D., Lee S. K. Zabbix Mastering. Packt Publ., 2013. 358 p.

17. Nagios: отраслевой стандарт мониторинга ИТ-инфраструктуры. – URL: https://www.nagios.org/, 2019 (дата обращения 03.07.2021).

18. XGU: Cacti. – URL: http://xgu.ru (дата обращения 03.07.2021).

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

20. Аллакин В. В. Формирование сервера мониторинга функциональной безопасности информационно-телекоммуникационной сети общего

пользования на основе оценки SRE-метрик // Техника средств связи. 2021. № 1 (153). С. 77-85.

21. Сторожук М. Использование систем мониторинга сетей для обеспечения работы критически важных приложений // Первая миля. 2021. № 1. С. 40-44.

22. Голубцов В., Федоренко М. Сервисно-ресурсная модель. От теории к практике. – URL: https://www.osp.ru/itsm/2012/09/13017362.html (дата обращения 21.07.2021).

23. 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).

24. Соглашение об уровне сервиса или что такое SLA (Service Level Agreement) – URL: http://www.wellink.ru/content/SLA-service-level-agreement (дата обращения 21.07.2021).

25. Бакланов И. Г. Оправдание OSS. – М.: Издательские решения, 2016. – 131 с.

26. Amazon, «Amazon CloudWatch». – URL: https://aws.amazon.com/cloudwatch (дата обращения 03.07.2021).

27. Montes H., Sanchez A., Memishi B., Perez M. S., António G. Gmone: an integrated approach to cloud monitoring. Future Generation Computer Systems, 2013, vol. 29, no. 8, pp. 2026-2040 (дата обращения 03.07.2021).

28. De Chavez S. A., Uriarte R. B., Westfall K. B. Towards an architecture for Monitoring Private Clouds. IEEE Communications Magazine. 2011, vol. 49, no. 12, pp. 130-137.

29. IBM, «IBM Tivoli Monitoring». – URL: https://www.ibm.com/support/knowledgecenter/en/SS3JRN_7.2.0/com.ibm.itm.doc/itm_install06.htm (дата обращения 03.07.2021).

30. HP BTO OpenView. – URL: http://www.hp.com/hpinfo/newsroom/press_kits /2010/HPSoftwareUniverseBarcelona2010/HP_Applications_Portfolio_brochure.pdf (дата обращения 03.07.2021).

31. Alcaraz Calero J. M., Aguado J. G. Monpaas: Adaptive Monitoring Platform as a Service for Cloud Computing Infrastructures and Services. IEEE Transactions on Services Computing, 2015, vol. 8, no 1, pp. 65-78.

32. 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).

33. Kenneth R., Sheers HP OpenView Event Correlation Services // Hewlett-Packard Journal. 1996. Article 4. P. 1-10. [Электронный ресурс]. – URL: http://www.hpl.hp.com/hpjournal/96oct/oct96a4.pdf (дата обращения 03.07.2021).

34. Hachey G. Instant Open NMS Starter. Birmingham: Packt Publ., 2013. 60 p.

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

36. Игнатов Н. А. Прогнозирование временных рядов с регулярными циклическими компонентами с помощью модели периодически

коррелированных случайных процессов // Научные труды: Институт народнохозяйственного прогнозирования РАН, 2011. С. 461-477.

37. Батурин А. Прогноз по методу экспоненциального сглаживания с трендом и сезонностью Хольта-Винтерса [Электронный ресурс] – URL: https://4analytics.ru/prognozirovanie (дата обращения 03.07.2021).

38. Яковлева А. В. Эконометрика. Конспект лекций. М.: ЭКСМО, 2008. 244 с.

39. Кашкин В. Б., Рублева Т. В. Применение сингулярного спектрального анализа для выделения слабо выраженных трендов // Известия Томского политехнического университета. 2007. Т. 311. № 5. С. 116-119.

40. Нашивочников Н. В., Пустарнаков В. Ф. Топологические методы анализа в системах поведенческой аналитики // Вопросы кибербезопасности. 2021. № 2. С. 26-36.

41. Макаренко Н. Г. Эмбедология и нейропрогноз. Ч. 1. – М. МИФИ. 2003. – 188 с.

42. Krakovska A., Mezeiova K., Budacova N. Use of False Nearest Neighbours for Selecting Variables and Embedding Parameters for State Spase Reconstruction // Journal of Complex Systems. 2015. pp. 1-12. – URL: https//doi:org/10.1155/2015/932750 (дата обращения 03.07.2021).

43. Пичкалев А. В. Применение кривой желательности Харрингтона для сравнительного анализа автоматизированных систем контроля // Вестник Красноярсконо государственного технического университета. 1997. № 1. С. 128-132.

44. Arjovsky M., Chintala S., Bottou L. Wasserstein Generative Adversarial Networks // Proceedings of the 34th International Conference on Machine Learning, PMLR. 2017. Pp. 214-223.

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

46. Kotenko I., Saenko I., Ageev S. Applying Fuzzy Computing Methods for On-line Monitoring of New Generation Network Elements // Advances in Intelligent Systems and Computing. 2018. Vol. 874. Springer, Cham. Pp. 331-340.

47. Kotenko I., Saenko I., Ageev S. Monitoring the State of Elements of Multi-service Communication Networks on the Basis of Fuzzy Logical Inference // Proceedings of the Sixth International Conference on Communications. Computation, Networks and Technologies (INNOV-2017). 2017. Pp. 26-32.

48. Kotenko I. V., Budko P. A., Vinogradenko A. M., Saenko I. B. An Approach for Intelligent Evaluation of the State of Complex Autonomous Objects Based on the Wavelet Analysis // The 18th International conference on intelligent software methodologies, tools and techniques (SOMET'2019) – Kuching, Sarawak, Malaysia, 23-25 September 2019. Pp. 25-38.

49. Грабуст П. Способы оценок сходства временных рядов // Научные труды Международной НТК «Теория вероятностей, случайные процессы, математическая статистика и приложения», Минск, БГУ, 15-19 сентября 2008 г. Минск: Белорусский государственный университет, 2008. С. 23-24.

50. Ульянов М. В., Сметанин Ю. Г. Об одном подходе к построению кластерного пространства временных рядов: колмогоровская и гармоническая

сложность // Proceedings of the International scientific-practical conference «Information Control Systems and Technologies» (ICST 2013). Odessa, 2013. С. 30-36.

51. 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, UK. 2017 DOI: 10.23919/INM.2017.7987291 (дата обращения 30.07.2021).

52. Сметанин Ю. Г., Ульянов М. В. Мера символьного разнообразия: подход комбинаторики слов к определению обобщенных характеристик временных рядов // Бизнес-информатика. 2014. № 3 (29). С. 40-48.

53. Обзор рынка систем поведенческого анализа // User and Entity Behavioral Analytics (UBA/UEBA) 23 ноября 2017. – URL: https://www.anti-malware.ru /analytics /Market_Analysis/user-and-entity-behavioral-analytics-ubaueba (дата обращения 04.07.2021).

54. Сухопаров М. Е., Лебедев И. С. Модели анализа функционального состояния элементов устройств сетей и телекоммуникаций «Индустрии 4.0»: монография. – СПб.: Политех-Пресс, 2020. – 121 с.

55. Нашивочников Н. В., Большаков А. А., Николашин Ю. А., Лукашин А. А. Проблемные вопросы применения аналитических средств безопасности киберфизических систем предприятий ТЭК // Вопросы кибербезопасности. 2019. № 5 (33). С. 26-33.

56. Альперович М. Введение в OLAP и многомерные базы данных. – URL: http://www.olap.ru/basic/alpero2i.asp (дата обращения 04.07.2021).

57. Воронков К. Л., Григорьева А. И., Шерстюк Ю. М. Автоматизация описания и построения многомерных кубов данных // X Санкт-Петербургская международная конференция «Региональная информатика – 2006 (РИ-2006)», Санкт-Петербург, 24-26 октября 2006 г.: Материалы конференции. – СПб.: СПОИСУ, 2006. – С. 28-29.

58. Воронков К. Л., Григорьева А. И., Шерстюк Ю. М. Организация сбора и использование ретроспективных данных мониторинга средств телекоммуникаций // X Санкт-Петербургская международная конференция «Региональная информатика – 2006 (РИ-2006)», Санкт-Петербург, 24-26 октября 2006г.: Материалы конференции. – СПб.: СПОИСУ, 2006. – С. 77.

59. Подиновский В. В. Идеи и методы теории важности критериев в многокритериальных задачах принятия решений. – М.: Наука, 2019. – 103 с.

60. Васильев Н. В., Забродин О. В., Яшин А. И. Автоматизированный программный комплекс оценки качества обслуживания в телекоммуникационной сети // Техника средств связи. 2018. № 3 (143). С. 56-61.

61. Holleczek T. Statistical Analysis of IP Performance Metrics in International Research and Educational Networks. Nuremberg. ETSI. 2008. Pp. 105-114.

62. Сметанин Ю. Г., Ульянов М. В. Энтропийные характеристики разнообразия в символьном представлении временных рядов // Современные информационные технологии и ИТ-образование. 2014. № 10. С. 426-436.

63. Орлов Ю. Л. Компьютерная реализация оценок сложности текстов // Материалы Российской НТК «Дискретный анализ и исследование операций» (ДАОР), Новосибирск, Институт математики СО РАН, 28 июня – 2 июля 2004. Новосибирск: Издательствово Институтата математики СО РАН, 2004. С. 225.

64. Математические методы для анализа последовательностей ДНК. – М.: Мир, 1999. – 349 с.

65. Ульянов М. В., Сметанин Ю. Г. Подход к определению характеристик колмогоровской сложности временных рядов на основе символьных описаний // Бизнес-информатика. 2013. № 2. С. 49-54.

66. Петрушин В. Н., Ульянов М. В. Бикритериальный метод построения гистограмм // Информационные технологии и вычислительные системы. 2012. № 4. С. 22–31.

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

68. Aho A. V., Corasick M. J. Efficient string matching: An aid to bibliographic search // Communications of the ACM. 1975. Vol. 18. no. 6. Pp. 333-340. DOI: 10.1145/360825.360855.

69. Lind D., Marcus B. An introduction to symbolic dynamics and coding. – Cambridge, UK: Cambridge University Press, 1995. – 495 p.

70. Королёв В. Ю. EM-алгоритм, его модификации и их применение к задаче разделения смесей вероятностных распределений. Теоретический обзор. – М.: ИПИРАН, 2007. – 94 с.

71. Клейнрок Л. Вычислительные сети с очередями. – М.: Мир, 1979. – 600 с.

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

73. Таненбаум Э., Бос Х. Современные операционные системы. – СПб.: Питер, 2018. – 1120 с.

74. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2018. – 960 с.

75. ITU-T Recommendations ITU-T Y. 1540 (07.2016). Служба передачи данных по межсетевому протоколу (IP) – Параметры рабочих характеристик переноса и доступности IP-пакетов – URL: http://handle.itu.int/11.1002/1000/12975 2016-07-29 (дата обращения 14.07.2021).

76. ITU-T Recommendations M.2301 (07.2002). Требуемые рабочие характеристики и процедуры для обеспечения и технического обслуживания сетей на базе IP. – URL: http://handle.itu.int/11.1002/1000/6079 2002-07-14 (дата обращения 14.07.2021).

77. Bunke H., Dickinson P. J., Kraetzl M., Wallis W. D. A Graph-Theoretic Approach to Enterprise Network Dynamics. – Basel: Birkhauser, 2007. – 226 p.

78. Shoubridge P., Kraetzl M., Wallis W. D., Bunke H. Detection of abnormal change in time series of graphs // Journal of Interconnection Networks. 2002. no. 3 (1&2). Pp. 85–101.

79. Wallis W. D., Shoubridge P. J., Kraetzl M., Ray D. Graph distances using graph union. Pattern Recognition Letters, 2001, no. 22. Pp. 701–704.

80. Parkes D. D., Wallis W. D. Graph Theory and the Study of Activity Structure. Timing Space and Spacing Time, vol. 2: Human Activity and Time Geography. Edward Arnold, London, 1978.

81. Umeyama S. An eigendecomposition approach to weighted graph matching problems // IEEE Transactions on Pattern Recognition and Machine Intelligence. 1988. no. 10 (5). Pp.695–703.

82. Цветкович Д., Дуб М., Захс Х. Спектры графов. Теория и применение. – Киев: Наукова думка, 1984. – 384 с.

References

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

2. ITU-T: General principles and general reference model for Next Generation Networks. Recommendation Y. 2011. Geneva, 2004. Available at: https://www.itu.int/rec/T-REC-Y.2011-200410-I/en (accessed 30 July 2021).

3. 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. Available at: https//doi:10.23919/INM.2017.7987291 (accessed 30 July 2021).

4. Budko P. A. *Upravlenie resursami informacionno-telekommunikacion-nyh sistem. Metody optimizacii* [Resource management of Information and Telecommunications Systems. Optimization methods]. St. Petersburg, Military Academy of Communications Publ., 2012. 512 p. (in Russian).

5. 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).

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

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

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

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

10. Legkov K. E., Baboshin V. A., Nesterenko O. E. Modeli i metody upravleniya sovremennymi multiservisnymi setyami svyazi [Models and methods of management of the modern multiservice networks]. *Means of Communication Equipment*. 2018, no. 2 (142), pp. 181-182 (in Russian).

11. Legkov K. E. Protsedury i vremennyye kharakteristiki operativnogo upravleniya trafikom v transportnoy seti spetsialnogo naznacheniya paketnoy kommutatsii [Procedures and temporal characteristics of the operational management

of traffic in the transport network of the special purpose packet switching]. *T-Comm – Telecommunications and Transport*, 2012, vol. 6, pp. 42-46 (in Russian).

12. 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).

13. Novyj podhod k obucheniyu setevym tekhnologiyam. Izuchenie setevogo oborudovaniya Cisco, protokolov i mekhanizmov posredstvom postroeniya krupnoj korporativnoj seti [A new approach to learning network technologies. Study of Cisco network equipment, protocols and mechanisms by building a large corporate network]. – URL: https://www.darkmaycal-it.ru/cisco/ (accessed 03 July 2021) (in Russian).

14. 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).

15. TechNet Magazine: System Center Operations Manager 2012: Prostota rasshireniya vozmozhnostej monitoringa [System Center Operations Manager 2012: it's Easy to extend monitoring capabilities]. Available at: http://technet.microsoft.com (accessed 03 July 2021) (in Russian).

16. Vacche A. D., Lee S. K. Zabbix Mastering. Packt Publ., 2013. 358 p.

17. Nagios: otraslevoj standart monitoringa IT-infrastruktury [an industry standard for monitoring IT infrastructure]. Available at: https://www.nagios.org/, 2019 (accessed 03 July 2021) (in Russian).

18. XGU: Cacti. – URL: http://xgu.ru (accessed 03 July 2021).

19. 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, 2005. 264 p. (in Russian).

20. Allakin V. V. Formation of a server for monitoring the functional security of a public information and telecommunications network based on the evaluation of SRE-metrics. *Means of Communication Equipment*, 2021, no. 1 (153), pp. 77-85 (in Russian).

21. Storozhuk M. The use of network monitoring systems to ensure the operation of critical applications. *The first mile*, 2021, no. 1, pp. 40-44 (in Russian).

22. Golubtsov V., Fedorenko M. Servisno-resursnaya model'. Ot teorii k praktike [Service-resource model. From theory to practice]. Available at: https://www.osp.ru/itsm/2012/09/13017362.html (accessed 21 July 2021) (in Russian).

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

24. Soglashenie ob urovne servisa ili chto takoe SLA (Service Level Agreement) [Agreement about the level of service or what is SLA (Service Level Agreement)]. Available at: http://www.wellink.ru/content/SLA-service-level-agreement (accessed 21 July 2021) (in Russian).

25. Baklanov I. G. *Opravdanie OSS* [Justification OSS]. Moscow, Publishing solutions, 2016. 131 p. (in Russian).

26. Amazon, «Amazon CloudWatch». Available at: https://aws.amazon.com/cloudwatch (accessed 03 July 2021).

27. Montes H., Sanchez A., Memishi B., Perez M. S., António G. Gmone: an integrated approach to cloud monitoring. Future Generation Computer Systems, 2013, vol. 29, no. 8, pp. 2026-2040 (accessed 03 July 2021).

28. De Chavez S. A., Uriarte R. B., Westfall K. B. Towards an architecture for Monitoring Private Clouds. *IEEE Communications Magazine*, 2011, vol. 49, no. 12, pp. 130-137.

29. IBM, "IBM Tivoli Monitoring". Available at: https://www.ibm.com/support/knowledgecenter/en/SS3JRN_7.2.0/com.ibm.itm.doc/itm_install06.htm (accessed 0321 July 2021).

30. HP BTO OpenView. Available at: http://www.hp.com/hpinfo/newsroom /press_kits/2010/HPSoftwareUniverseBarcelona 2010/HP_Applications_Portfolio _brochure. pdf, 2019 (accessed 03 July 2021).

31. Alcaraz Calero J. M., Aguado J. G. Monpaas: Adaptive Monitoring Platform as a Service for Cloud Computing Infrastructures and Services. *IEEE Transactions on Services Computing*, 2015, vol. 8, no 1, pp. 65-78.

32. 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 03.07.2021) (in Russian).

33. Kenneth R., Sheers HP OpenView Event Correlation Services. *Hewlett-Packard Journal*, 1996, Article 4. P. 1-10. Available at: http://www.hpl.hp.com/hpjournal/96oct/ oct96a4.pdf (accessed 03 July 2021).

34. Hachey G. Instant Open NMS Starter. Birmingham, Packt Publ., 2013. 60 p.

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

36. Ignatov N. A. Prognozirovanie vremennyh ryadov s regulyarnymi ciklicheskimi komponentami s pomoshch'yu modeli periodicheski korrelirovannyh sluchajnyh processov [Prediction of time series with regular cyclical components using the model of a periodically correlated random processes]. *Nauchnye trudy: Institut narodnohozyajstvennogo prognozirovaniya RAN* [proceedings of the Institute of economic forecasting of the Russian Academy of Sciences], 2011, pp. 461-477 (in Russian).

37. Baturin A. Prognoz po metodu eksponencial'nogo sglazhivaniya s trendom i sezonnost'yu Hol'ta-Vintersa [Forecast using exponential smoothing with trend and seasonality Holt-winters]. Available at: https://4analytics.ru/prognozirovanie (accessed 03 July 2021) (in Russian).

38. Yakovleva A. V. *Ekonometrika* [Econometrics]. Moscow, EKSMO, 2008. 244 p. (in Russian).

39. Kashkin V. B., Rubleva T. V. Primenenie singulyarnogo spektral'nogo analiza dlya vydeleniya slabo vyrazhennyh trendov [Application of singular spectral

analysis for the identification of weakly expressed trends]. *Bulletin of the Tomsk Polytechnic University*, 2007, vol. 311, no. 5, pp. 116-119 (in Russian).

40. Nashivochnikov N. V., Pustarnakov V. F. Topologicheskie metody analiza v sistemah povedencheskoj analitiki [Topological methods of analysis in behavioral analytics systems]. *Voprosy kiberbezopasnosti*, 2021, no. 2, pp. 26-36 (in Russian).

41. Makarenko N. G. *Embedologiya i nejroprognoz. Ch. 1*. [Embedology and neuroprognosis. Part 1]. Moscow, Moscow Engineering Physics Institute Publ., 2003. 188 p. (in Russian).

42. Krakovska A., Mezeiova K., Budacova N. Use of False Nearest Neighbours for Selecting Variables and Embedding Parameters for State Spase Reconstruction. *Journal of Complex Systems*, 2015, pp. 1-12. Available at: https://doi.org/10.1155/2015/932750 (accessed 03 July 2021).

43. Pichkalev A. V. Primenenie krivoj zhelatel'nosti Harringtona dlya sravnitel'nogo analiza avtomatizirovannyh sistem kontrolya [Application of the Harrington desirability curve for comparative analysis of utomated control systems]. *Vestnik of the Krasnoyarsk State Technical University*, 1997, no. 1, pp. 128-132 (in Russian).

44. Arjovsky M., Chintala S., Bottou L. Wasserstein Generative Adversarial Networks. *Proceedings of the 34th International Conference on Machine Learning*, PMLR. 2017. Pp. 214-223.

45. 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).

46. Kotenko I., Saenko I., Ageev S. Applying Fuzzy Computing Methods for On-line Monitoring of New Generation Network Elements. *Advances in Intelligent Systems and Computing*, 2018, vol. 874, pp. 331-340.

47. Kotenko I., Saenko I., Ageev S. Monitoring the State of Elements of Multi-service Communication Networks on the Basis of Fuzzy Logical Inference. *In: Proceedings of the Sixth International Conference on Communications. Computation, Networks and Technologies (INNOV-2017)*. 2017, pp. 26-32.

48. Kotenko I. V., Budko P. A., Vinogradenko A. M., Saenko I. B. An Approach for Intelligent Evaluation of the State of Complex Autonomous Objects Based on the Wavelet Analysis. *The 18th International conference on intelligent software methodologies, tools and techniques (SOMET'2019)*. Kuching, Sarawak, Malaysia, 23-25 September 2019, pp. 25-38.

49. Grobust P. Sposoby ocenok skhodstva vremennyh ryadov [Methods of evaluations of the similarity of time series]. *Nauchnye trudy Mezhdunarodnoj NTK «Teoriya veroyatnostej, sluchajnye processy, matematicheskaya statistika i prilozheniya»* [*Proceedings of the International NTK "Theory of probability, stochastic processes, mathematical statistics and applications"*] 15-19 September 2008. Minsk, Belarusian state University, 2008, pp. 23-24 (in Russian).

50. Ulyanov M. V., Smets Y. G. Ob odnom podhode k postroeniyu klasternogo prostranstva vremennyh ryadov: kolmogorovskaya i garmonicheskaya slozhnost' [On one approach to the construction of a clustered space time series: Kolmogorov and harmonic complexity]. *Proceedings of the International scientific-practical*

conference "Information Control Systems and Technologies" (ICST 2013). Odessa, 2013. Pp. 30-36 (in Russian).

51. 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, UK. 2017 DOI:10.23919/INM.2017.7987291 (accessed 30 July 2021).

52. Smetanin Yu. G., Ulyanov M. V. Mera simvol'nogo raznoobraziya: podhod kombinatoriki slov k opredeleniyu obobshchennyh harakteristik vremennyh ryadov [a Measure of symbolic diversity: an approach to the combinatorics of words to identify generalized characteristics of time series]. *Business Informatics*, 2014, no. 3 (29), pp. 40-48 (in Russian).

53. Obzor rynka sistem povedencheskogo analiza [Market overview of behavioral systems analysis, User and Entity Behavioral Analytics] (UBA/UEBA) November 23, 2017. Available at: https://www.anti-malware.ru/analytics/Market _Analysis/user and entity behavioral analytics-ubaueba (accessed 04 July 2021) (in Russian).

54. Suhoparov M. E., Lebedev I. S. *Modeli analiza funkcional'nogo sostoyaniya elementov ustrojstv setej i telekommunikacij «Industrii 4.0»* [Model analysis of the functional state of the elements of the devices, networks and telecommunications Industry 4.0]. St. Petersburg, Polytechnic Press, 2020. 121 p. (in Russian).

55. Nashivochnikov N. V., Bolshakov A. A., Nikolashin Yu. A., Lukashin A. A. Problemnye voprosy primeneniya analiticheskih sredstv bezopasnosti kiberfizicheskih sistem predpriyatij TEK [Problematic issues of the use of analytical security tools for cyber-physical systems of fuel and energy complex enterprises]. *Voprosy kiberbezopasnosti*, 2019, no. 5 (33), pp. 26-33 (in Russian).

56. Alperovich M. Vvedenie v OLAP i mnogomernye bazy dannyh [Introduction to OLAP and multidimensional databases]. Available at: http://www.olap.ru/basic/alpero2i.asp (accessed 04 July 2021) (in Russian).

57. Voronkov K. L., Grigorieva A. I., Sherstyuk Yu. M. Avtomatizaciya opisaniya i postroeniya mnogomernyh kubov dannyh [Automation of description and construction of multidimensional data cubes]. *X Sankt-Peterburgskaya mezhdunarodnaya konferenciya «Regional'naya informatika – 2006 (RI-2006)»* [X St. Petersburg International Conference "Regional Informatics-2006 (RI-2006)"], St. Petersburg, October 24-26, 2006. Conference materials. St. Petersburg, St. Petersburg Society of Informatics, Computer Technology, Communication and Control Systems, 2006, pp. 28-29 (in Russian).

58. Voronkov K. L., Grigorieva A. I., Sherstyuk Yu. M. Organizaciya sbora i ispol'zovanie retrospektivnyh dannyh monitoringa sredstv telekommunikacij [Organization of the collection and use of retrospective data for monitoring telecommunications facilities]. *X Sankt-Peterburgskaya mezhdunarodnaya konferenciya «Regional'naya informatika – 2006 (RI-2006)»* [X St. Petersburg International Conference "Regional Informatics-2006 (RI-2006)"], St. Petersburg, October 24-26, 2006. Conference materials. St. Petersburg, St. Petersburg Society of Informatics, Computer Technology, Communication and Control Systems, 2006, pp. 77 (in Russian).

59. Podinovsky V. V. *Idei i metody teorii vazhnosti kriteriev v mnogokriterial'nyh zadachah prinyatiya reshenij* [Ideas and methods of the theory of the importance of criteria in multi-criteria decision-making problems]. Moscow. Nauka Publ., 2019. 103 p. (in Russian).

60. Vasiliev N. V., Zabrodin O. V., Yashin A. I. Avtomatizirovannyj programmnyj kompleks ocenki kachestva obsluzhivaniya v telekommunikacionnoj seti [Automated software package for assessing the quality of service in a telecommunications network]. *Means of Communication Equipment*, 2018, no. 3 (143), pp. 56-61 (in Russian).

61. Holleczek T. *Statistical Analysis of IP Performance Metrics in International Research and Educational Networks*. Nuremberg, ETSI, 2008, pp. 105-114.

62. Smetanin Yu. G., Ulyanov M. V. Entropijnye harakteristiki raznoobraziya v simvol'nom predstavlenii vremennyh ryadov [Entropic characteristics of diversity in the symbolic representation of time series]. *Sovremennye informacionnye tekhnologii i IT-obrazovanie* [Modern information technologies and IT education], 2014, no. 10, pp. 426-436 (in Russian).

63. Orlov Yu. L. Komp'yuternaya realizaciya ocenok slozhnosti tekstov [Computer implementation of text complexity estimates]. *Materialy Rossijskoj NTK «Diskretnyj analiz i issledovanie operacij» (DAOR), Novosibirsk, Institut matematiki SO RAN* [Materials of the Russian STC "Discrete Analysis and Operations Research" (DAOR). Novosibirsk, Institute of Mathematics SB RAS]. June 28-July 2, 2004. Novosibirsk: Publishing house of the Institute of Mathematics SB RAS, 2004. 225 p. (in Russian).

64. *Matematicheskie metody dlya analiza posledovatel'nostej DNK* [Mathematical methods for analyzing DNA sequences]. Moscow, Mir, 1999. 349 p. (in Russian).

65. Ulyanov M. V., Smetanin Yu. G. Podhod k opredeleniyu harakteristik kolmogorovskoj slozhnosti vremennyh ryadov na osnove simvol'nyh opisanij [An approach to determining the characteristics of the Kolmogorov complexity of time series based on symbolic descriptions]. *Business Informatics*, 2013, no. 2, pp. 49-54 (in Russian).

66. Petrushin V. N., Ulyanov M. V. Bikriterial'nyj metod postroeniya gistogramm [Bicriteria method of constructing histograms]. *Informatsionnye tekhnologii i vychislitelnye sistemy*, 2012, no. 4, pp. 22-31 (in Russian).

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

68. Aho A. V., Corasick M. J. Efficient string matching: An aid to bibliographic search. *Communications of the ACM*, 1975, vol. 18, no. 6, pp. 333-340. DOI:10.1145/360825.360855.

69. Lind D., Marcus B. *An introduction to symbolic dynamics and coding*. Cambridge, UK. Cambridge University Press, 1995. 495 p.

70. Korolev V. Yu. *EM-algoritm, ego modifikacii i ih primenenie k zadache razdeleniya smesej veroyatnostnyh raspredelenij. Teoreticheskij obzor*. [EM-algorithm, its modifications and their application to the problem of separation of mixtures of probability distributions. Theoretical review]. Moscow, Institute of

Computer Science Problems of the Russian Academy of Sciences Publ., 2007. 94 p. (in Russian).

71. Kleinrock L. Queueing Systems: Volume II – Computer Applications. New York: Wiley Interscience, 1975. 576 p.

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

73. Tanenbaum E., Bos H. *Sovremennye operacionnye sistemy* [Modern operating systems]. St. Petersburg, Peter Publ., 2018. 1120 p. (in Russian).

74. Tanenbaum E., Weatherall D. *Komp'yuternye seti* [Computer networks]. St. Petersburg, Peter Publ., 2018. 960 p. (in Russian).

75. ITU-T Recommendations ITU-T Y. 1540 (07.2016). Sluzhba peredachi dannyh po mezhsetevomu protokolu (IP) – Parametry rabochih harakteristik perenosa i dostupnosti IP-paketov [Data transmission service over the Internet Protocol (IP) – Parameters of the performance characteristics of the transfer and availability of IP packets]. Available at: http://handle.itu.int/11.1002/1000/12975 2016-07-29 (accessed 14 July 2021) (in Russian).

76. ITU-T Recommendations M. 2301 (07.2002). Trebuemye rabochie harakteristiki i procedury dlya obespecheniya i tekhnicheskogo obsluzhivaniya setej na baze IP [Required performance characteristics and procedures for providing and maintaining IP]. Available at: http://handle.itu.int/11.1002/1000/6079 2002-07-14 (accessed 14 July 2021) (in Russian).

77. Bunke H., Dickinson P. J., Kraetzl M., Wallis W. D. *A Graph-Theoretic Approach to Enterprise Network Dynamics*. Basel, Birkhauser, 2007. 226 p.

78. Shoubridge P., Kraetzl M., Wallis W. D., Bunke H. Detection of abnormal change in time series of graphs. *Journal of Interconnection Networks*, 2002, no. 3 (1&2), pp. 85–101.

79. Wallis W. D., Shoubridge P. J., Kraetzl M., Ray D. Graph distances using graph union. *Pattern Recognition Letters*, 2001, no. 22, pp. 701–704.

80. Parkes D. D., Wallis W. D. *Graph Theory and the Study of Activity Structure. Timing Space and Spacing Time*, vol. 2: Human Activity and Time Geography. Edward Arnold, London, 1978.

81. Umeyama S. An eigendecomposition approach to weighted graph matching problems. *IEEE Transactions on Pattern Recognition and Machine Intelligence*, September 1988, no. 10 (5), pp. 695-703.

82. Tsvetkovich D., Dubh M., Sachs H. *Spektry grafov. Teoriya i primenenie* [Spectra of graphs. Theory and application]. Kiev, Naukova dumka Publ., 1984. 384 p. (in Russian).

Статья поступила 15.08.2021 г.

Информация об авторах

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

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

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, 9, корп. 1, кв. 252.

Васильев Николай Владимирович – кандидат технических наук. Начальник сектора. Публичное акционерное общество «Информационные телекоммуникационные технологии». Область научных интересов: мониторинг информационных ресурсов; сбор и обработка информации. E–mail: gandvik1984@gmail.com

Адрес: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

A general approach to the construction of advanced monitoring systems for distributed information and telecommunications networks

V. V. Allakin, N. P. Budko, N. V. Vasiliev

Task statement: *based on a review of existing technologies and existing monitoring systems for public information and telecommunications networks, as well as an analysis of the scientific and methodological apparatus for evaluating the time series of observed metrics, to develop general requirements and approaches to building promising network monitoring systems and to develop a methodology for predicting (preventive identification) of abnormal situations based on the results of monitoring the functional state of network elements.* ***The purpose of the work:*** *to develop a general approach to the formation of methods for predicting the state of connections on a public information and telecommunications network, as well as its network devices. Methods used: methods of multidimensional data analysis; methods of cluster analysis; topological methods of time series analysis; methods of behavioral analytics; symbolic representation of time series; network monitoring technologies Site/System Reliability Engineering, as a set of engineering practices that support reliable and trouble-free operation of applications in the present and future; Operation Support Systems, as a technology for supporting operations; methods of system analysis, structural synthesis, forecast theory, diagnostic theory, classification theory.* ***The novelty of the work:*** *to increase the stability and reliability of a controlled heterogeneous information and telecommunications network, the key architectural principle of designing its monitoring subsystem is the principle of distribution and decentralization. Preventive identification of abnormal states of network elements (in the form of devices, channels, paths and routes) is proposed to be carried out by identifying "forbidden" code combinations when observing time series, which are processed by symbolic dynamics methods borrowed from bioinformatics, previously used in the analysis of complex nucleotide genomic sequences, as well as by introducing a special monitoring mode, when, when identifying a pre-failure technical condition, the accuracy of the survey by the monitoring server of the network element is significantly increased in order to timely take preventive control actions on the network infrastructure and prevent the failure of the network element or the occurrence of an accident on the network. A method for classifying the state of network elements is proposed, consisting of a stage of training a classifier based on an EM algorithm, as well as a stage of directly classifying the type of technical condition.* ***Result:*** *the paper proposes a generalized architecture for building promising network monitoring systems, as well as a general subject-object model of it in the form of "entity-connection". The functions of the network monitoring subsystem and the monitoring server as its key element are defined. A variant of the monitoring server structure is considered. The assigned monitoring objects are defined, as well as a list of metric data collected from them from the point of view of the functional performance of the network. The method of symbolic representation of time series is chosen, on the basis of which the entropy of code words*

describing the time series of the observed metric of a functioning network element is estimated, and an algorithm for identifying its anomalous state on a time series of parameters is developed, consisting of four stages: the preliminary stage, the stage of encoding time series, the stage of identifying the type of technical condition of the network element and the final stage. ***Practical significance:*** *A general approach to the construction of an algorithm for the functioning of promising network monitoring systems has been developed.*

Keywords: *time series, monitoring decentralization, information and telecommunications network, network monitoring subsystem, monitoring server.*

Information about Authors

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

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

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.

Nikolay Vladimirovich Vasiliev – Ph.D. of Engineering Sciences. The head of the sector. Public Joint Stock Company "Information Telecommunications Technologies". Field of research: information monitoring; data acquisition. E–mail: gandvik1984@gmail.com

Address: 197342, Russia, St. Petersburg, 8 Kantemirovskaya St.