Научно-технический журнал

ТЕХНИКА СРЕДСТВ СВЯЗИ

MEANS OF COMMUNICATION EQUIPMENT

Scientific and Technical Journal

№ 2 (154) – 2021

РЕДАКЦИЯ: Верстка принт-макета: **Мамончикова А.С.**
Дизайн обложки: **Шаутин Д.В.**
Поддержка сетевой версии журнала: **Лебедев Д.А.**
Секретарь редакции: **Михайлова Н.В.**

АДРЕС РЕДАКЦИИ: 197342. Россия. г. Санкт-Петербург, ул. Кантемировская, дом 8,
Телефон: +7(812) 542-90-54; +7(812) 448-95-97; +7(812) 448-96-84
Факс: +7(812) 542-18-49. E-mail: intelteh@inteltech.ru.
Официальный сайт: www.inteltech.ru; www.mce-journal.ru

Научно-технических журнал
ТЕХНИКА СРЕДСТВ СВЯЗИ
MEANS OF COMMUNICATION EQUIPMENT
Scientific and Technical Journal
№ 2 (154) – 2021

Научно-технический журнал «Техника средств связи» – это рецензируемое научное издание, в котором публикуются результаты научных исследований специалистов в области современных инфокоммуникационных технологий и автоматизированных систем управления, средств связи и информационной безопасности. Журнал является правопреемником издававшихся с 1959 года Министерством промышленности средств связи СССР всесоюзных журналов «Вопросы радиоэлектроники. Серия: Техника проводной связи» и «Вопросы специальной радиоэлектроники. Серия: Техника проводной связи». С 1975 года журнал издается под названием «Техника средств связи». Учредитель и издатель журнала: Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»). Адрес учредителя и издателя журнала: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

Периодичность выхода журнала 4 номера в год.

Публикация в журнале является научным печатным трудом. Основное содержание издания представляют собой научные статьи и научные обзоры.

Информация предназначена для детей старше 12 лет.

Журнал зарегистрирован как сетевое и печатное издания в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Свидетельства о регистрации средств массовой информации: ПИ № ФС 77 – 80135 и ЭЛ № ФС 77 – 80136 от 31.12.2020 г.

ISSN (print): 2782-2141

ISSN (online): 2782-2133

СОДЕРЖАНИЕ

CONTENTS

Рубрики журнала: Анализ новых технологий и перспектив развития техники средств связи • Системы управления • • Передача, прием и обработка сигналов • Системы связи и телекоммуникации • Перспективные исследования • • Вычислительные системы • Информационные процессы и технологии. Сбор, хранение и обработка информации • • Моделирование сложных организационно-технических систем • Вопросы обеспечения информационной безопасности • • Интеллектуальные информационные системы • Робототехнические системы • Электронные и радиотехнические системы • • Объекты интеллектуальной собственности и инновационные технологии в области разработки средств телекоммуникаций

ПЕРЕДАЧА, ПРИЕМ И ОБРАБОТКА СИГНАЛОВ

УДК 621.396.93

Скрытность сверхузкополосных сигналов

Куприянов А.И.

Аннотация. *В статье рассмотрены условия работы обнаружителя сигнала в составе радиоэлектронного средства. При этом дана оценка спектра анализируемого сигнала по показателям качества его обнаружения на шумовом фоне, обусловленном как собственными шумами приемника, так и внешним шумовым полем. Представлена структура автокорреляционного (энергетического) обнаружителя априори неизвестного сигнала. Приведена диаграмма обмена между ошибками первого и второго рода при энергетическом обнаружении сигнала. Определены рабочие характеристики согласованного и энергетического обнаружителей при различных уровнях вероятностей ложных тревог. Рассчитана величина проигрыша энергетического обнаружителя оптимальному обнаружителю известного сигнала. В результате исследования показано, что расширение спектра сигнала улучшает скрытность от средств разведки. Однако уменьшение полосы спектра информационного сигнала, ухудшающее скрытность, может быть скомпенсировано применением псевдослучайной перестройки несущей частоты от символа к символу, или даже чаще. Сама возможность постановки помехи, прицельной по частоте сигнала, обусловлена надежностью измерения этой частоты. Поэтому защита от такой помехи должна предусматривать меры противодействия разведки. Среди таких мер необходимо рассматривать и исследовать способы, основанные на дезинформации разведывательного приемника.*

Ключевые слова*: оптимальный энергетический обнаружитель сигнала, параметр накопления, скрытность радиосигнала, решающее устройство, широкополосный сигнал.*

Введение

Эффективность и даже сама возможность подавления систем связи средствами радиоэлектронной борьбы (РЭБ) определяется возможностью постановки прицельной помехи. Прежде всего – прицельной по несущей частоте и по ширине спектра подавляемого сигнала. Следовательно, оперативная радио- и радиотехническая разведка (РРТР) поддержки РЭБ должна максимально быстро и надежно обнаруживать сигнал и определять его параметры.

Средства РРТР для определения названных параметров формируют оценку спектра процесса в области своих интересов (рис. 1) и определяют оценку ширины полосы спектра сигнала, присутствующего в составе этого процесса, а несущую частоту – по оценке центра этой полосы.

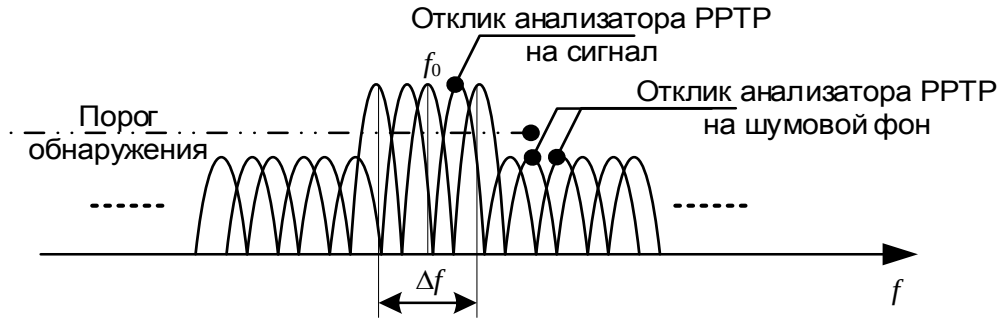


Рис. 1. Оценка спектра средством оперативной РРТР поддержки РЭБ

Таким образом, оценки Δf и f_0 и их качество в принципе определяются показателями качества обнаружения сигнала на шумовом фоне, обусловленном как собственными шумами приемника, так и внешним шумовым полем. А показатели качества обнаружения зависят, кроме прочего, от априорной параметрической неопределенности параметров для средства РРТР.

1. Моделирование энергетического обнаружителя радиоприемного устройства

Традиционно рассматриваемые модели параметрической неопределенности сигнала (полностью известный сигнал, сигнал с неизвестной фазой и флуктуирующей амплитудой, неизвестным временем прихода, неизвестной частотой) дают хорошее приближение при описании работы обнаружителей в радиолокационных и радионавигационных приемниках, в приемниках радиосистем передачи информации [1]. На основе этих моделей можно построить диаграммы обмена между вероятностями ошибок типа ложной тревоги и пропуска при различных соотношениях сигнал/шум в полосе обнаружителя. Но для средств разведки более характерен предельный случай ограниченности априорных данных о подлежащем обнаружению сигнале – полное их отсутствие. В такой ситуации средство разведки может выносить решение о наличии сигнала только на основании анализа его мощности P_u. Если мощность принимаемого колебания больше мощности собственного шумового фона, на входе приемника имеется сигнал.

Оценка мощности входного процесса

$$P^* = \frac{1}{T}\int_0^T u^2(t)\,dt \qquad (1)$$

формируется устройством, выполненным по схеме рис. 2.

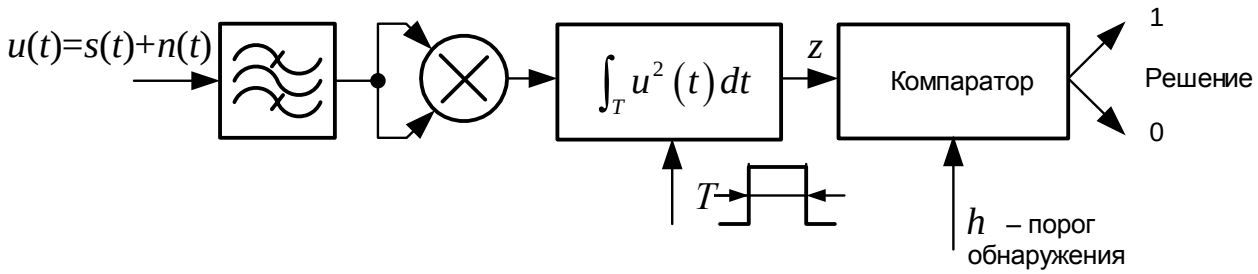


Рис. 2. Автокорреляционный (энергетический) обнаружитель априори неизвестного сигнала

Входное колебание фильтруется в полосе $\Delta f_ш$ и подается на схему обнаружителя, подобного корреляционному обнаружителю полностью известного сигнала. От корреляционного обнаружителя схема рис. 2 отличается тем, что, не имея образца сигнала, она в качестве опорного сигнала коррелятора использует само наблюдаемое на входе колебание $u(t)$.

Всю информацию о входном процессе $u(t)$ содержит выборка его дискретных значений, следующих через интервал времени $\Delta t = \frac{1}{\Delta f_ш}$. Поэтому объем выборки равен $\Delta f_ш T$. В результате накопления в интеграторе формируется величина z, такая, что

$$z = \begin{cases} \sum_{i=1}^{\Delta f_ш T} \frac{n_i^2}{\sigma^2} = \sum_{i=1}^{\Delta f_ш T} \frac{n_i^2}{P_ш} \text{ при отсутствии на входе сигнала, когда } s(t)=0, \\ \sum_{i=1}^{\Delta f_ш T} \frac{(n_i+s_i)^2}{\sigma^2} = \sum_{i=1}^{\Delta f_ш T} \frac{(n_i+s_i)^2}{P_ш+P_c} = \frac{1}{1+q}\sum_{i=1}^{\Delta f_ш T} \frac{(n_i+s_i)^2}{P_ш} \text{ при сигнале, когда } s(t)\neq 0, \end{cases} \qquad (2)$$

где $n_i = n(t - i\Delta t)$ и $s_i = s(t - i\Delta t)$ – дискретные по времени отсчеты входного шума и сигнала соответственно, $q = P_c/P_ш$.

Плотность распределения нормированного процесса z на выходе интегратора и, соответственно, на входе решающего устройства подчиняется закону χ^2 с $B = \Delta f_ш T$ числом степеней свободы:

$$W\left(z,\Delta f_{\text{ш}}T\right)=\begin{cases}\dfrac{z^{\frac{\Delta f_{\text{ш}}T}{2}-1}e^{-\frac{z}{2}}}{2\Gamma\left(\dfrac{\Delta f_{\text{ш}}T}{2}\right)} & \text{при } z\geq 0;\\ 0 & \text{при } z<0.\end{cases} \quad (3)$$

На рис. 3 представлены графики плотности распределения вероятностей квадратов входного нормального процесса для параметров накопления $\Delta f_{\text{ш}}T$ = 2, 10 и 20.

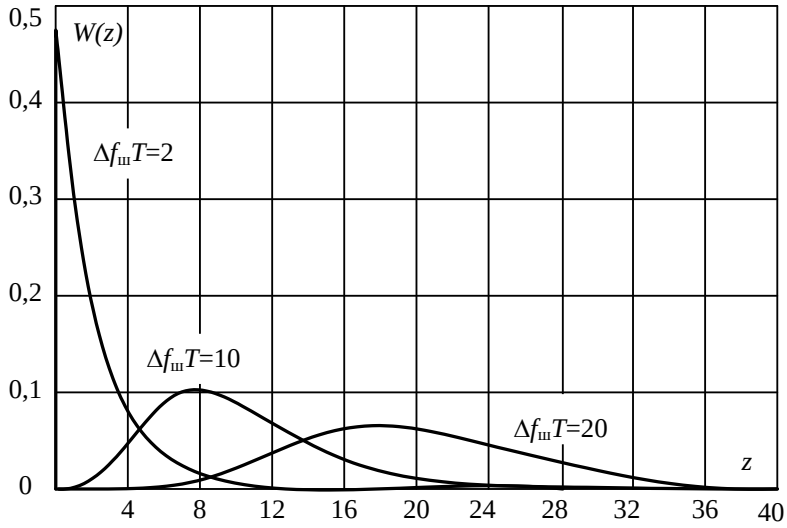


Рис. 3. Плотность распределения χ^2 с двумя, десятью и двадцатью степенями свободы

Как видно, распределение величины z, исходной для обнаружения сигнала приемником средства РРТР, существенно отличается от нормального для любых сколько-нибудь реальных соотношений входной полосы и полосы усредняющего фильтра после квадратора в энергетическом обнаружителе. Более детальный анализ показывает, что распределение χ^2 сходится к нормальному при $B \cong 30$ (и, разумеется, более). Соответственно, рабочие характеристики обнаружителя средства РРТР должны рассчитываться с учетом того, что распределение процесса на входе решающего устройства подчиняется не нормальному закону, как в обнаружителе радиолокатора, а χ^2.

Относительно величины $B = \Delta f_{\text{ш}}T$ необходимо принять следующие соглашения. Поскольку ширина спектра процесса на входе перемножителя (схемы возведения входного процесса в квадрат) равна $\Delta f_{\text{ш}}$, его отсчеты, следующие через интервал времени $\Delta t = \dfrac{1}{\Delta f_{\text{ш}}}$ некоррелированы, а для нормального шума – статистически независимы. Тогда за время наблюдения этого процесса (за время интегрирования T) будет накоплено $B = \Delta f_{\text{ш}}T$ независимых отсчетов. Выборка объемом B этих отсчетов содержат всю информацию о входном процессе. Поэтому, обрабатывая такую выборку, обнаружитель может реализовать наилучшие рабочие характеристики. В этом смысле B – мера информационной емкости процесса, с которым работает энергетический обнаружитель средства РРТР.

Если на входе совместно с шумом присутствует сигнал, то наилучшие условия для обнаружения сложатся тогда, когда входная полоса обнаружителя точно совпадет с его спектром («накроет» спектр сигнала, имеющего ширину Δf), а время интегрирования после перемножителя точно совпадет с интервалом времени существования сигнала T).

Если условия совпадения полос и времени не выполнены, часть энергии принимаемого сигнала будет потеряна, или энергия шума будет повышена. Поэтому характеристики обнаружения, естественно, будут хуже. Но по содержательному смыслу произведение $B = \Delta fT$ – это база обнаруживаемого сигнала.

Обычно в задачах синтеза и анализа алгоритмов обработки сигнала база характеризует возможность его сворачивания (сжатия) по времени и/или по частоте при когерентной обработке. В энергетическом приемнике, естественно, когерентная обработка не предусматривается. Сигнал рассматривается как чисто случайный процесс, а обнаружение происходит при сравнении с порогом мощности (точнее – энергии), присутствующего на входе колебания.

Таким образом, незнание базы и несущей частоты ограничивает объем априорных для средства разведки сведений о сигнале. Уменьшение объема этих сведений (неточность знания частоты, ширины спектра и длительности сигнала) может только ухудшить характеристики обнаружения. С другой стороны, дополнительные сведения о структуре сигнала, которые в принципе могли бы улучшить характеристики обнаружения, скорее всего, разведке недоступны. Характеристики приемника, учитывающего при работе больший объем априорной информации о структуре и параметрах сигнала, будут лучше, чем у энергетического, но только для того сигнала, с которым он согласован. Поэтому такой приемник не будет универсальным и не подойдет для использования средствами оперативной поддержки РЭБ.

Возможная адаптация приемника к параметрам обнаруживаемого сигнала требует времени. А потеря времени на адаптацию к неизвестным структуре и параметрам сигнала снизит характеристики обнаружения. Полученные при сделанных предположениях оценки качества энергетического приемника могут служить верхними, реалистическими оценками доступности сигнала для обнаружения техническими средствами разведки. Предположение о бóльших объемах доступной разведке априорной информации о сигнале и, следовательно, лучших характеристиках обнаружения, трудно обосновать. Предположения о более низкой априорной осведомленности могут привести к завышенным, чрезмерно оптимистическим оценкам скрытности сигналов радиоэлектронных средств (РЭС) от обнаружения средствами разведки.

2. Расчет рабочих характеристик энергетического обнаружителя

Используя приведенную выше модель χ^2 для распределения вероятностей процесса на входе решающего устройства энергетического обнаружителя, можно получить его рабочие характеристики. Считается, что решение о наличии сигнала обнаружитель принимает по критерию Неймана-Пирсона.

Порог обнаружения h в схеме рис. 2 определяется при заданном уровне вероятности ложных тревог решением уравнения

$$P_{\text{лт}} = \int_{h}^{\infty} W_{\text{ш}}\left(z, \Delta fT\right) dz = 1 - \int_{0}^{h} W_{\text{ш}}\left(z, \Delta fT\right) dz = 1 - F_{\text{ш}}\left(h, \Delta fT\right). \quad (4)$$

Откуда

$$h = F_{\text{ш}}^{-1}[(1 - P_{\text{лт}}),\ \Delta fT), \quad (5)$$

где $W_{\text{ш}}(z, \Delta fT)$ – плотность, а $F_{\text{ш}}(h, \Delta fT)$ – интегральная функция распределения вероятностей процесса на входе решающего устройства, соответствующая действию только шума на входе обнаружителя; $F_{\text{ш}}^{-1}(x, \Delta fT)$ – функция, обратная $F_{\text{ш}}(x, \Delta fT)$.

Вероятность правильного решения о наличии сигнала в полосе Δf на входе обнаружителя будет при этом равна

$$P_{\text{прав}} = \int_{h}^{\infty} W_{\text{с+ш}}\left(z, \Delta fT\right) dz = 1 - \int_{0}^{h} W_{\text{с+ш}}\left(z, \Delta fT\right) dz = 1 - F_{\text{с+ш}}\left(h, \Delta fT\right), \quad (6)$$

где $W_{\text{с+ш}}(z, \Delta fT)$ и $F_{\text{с+ш}}(h, \Delta fT)$ – соответственно плотность и интегральная функция условного распределения вероятностей процесса на входе решающего устройства, при условии присутствия на входе обнаружителя сигнала вместе с шумом.

Диаграммы обмена между $P_{\text{лт}}$ и $P_{\text{пр}} = 1 - P_{\text{прав}}$ для автокорреляционного (энергетического) обнаружителя изображены на рис. 4.

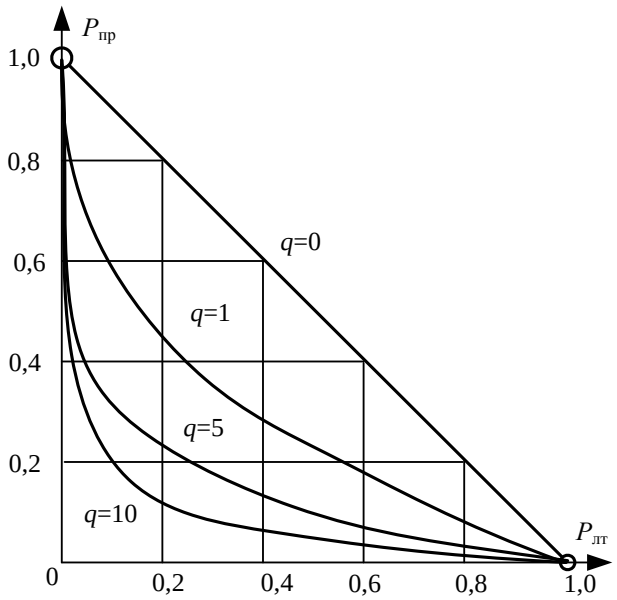


Рис. 4. Диаграмма обмена между вероятностями ошибок при энергетическом обнаружении

Поскольку считается, что обнаруживаемый сигнал не проявляет когерентных свойств, по действию на обнаружитель он подобен шуму. Поэтому рабочая характеристика обнаружителя определяется также как и при шуме с использованием распределения χ^2 с ΔfT степенями свободы, но при другом параметре масштаба:

$$W_{\text{с+ш}}\left(z, \Delta fT\right) = W_{\text{ш}}\left(\frac{z}{1+q}, \Delta fT\right) \quad (7)$$

и

$$\int_{0}^{h} W_{\text{с+ш}}\left(z, \Delta fT\right) dz = \int_{0}^{h} \frac{1}{1+q} W_{\text{с+ш}}\left(\frac{z}{1+q}, \Delta fT\right) dz = \int_{0}^{\frac{h}{1+q}} W_{\text{с+ш}}\left(t, \Delta fT\right) dt = F_{\text{ш}}\left(\frac{h}{1+q}, \Delta fT\right). \quad (8)$$

Откуда

$$P_{\text{прав}} = 1 - F_{\text{ш}}\left(\frac{h}{1+q}, \Delta fT\right). \quad (9)$$

Численный расчет рабочих характеристик энергетического обнаружителя в соответствии с (7)…(9) позволяет построить график рис. 5 для $P_{\text{лт}} = 10^{-3}$ и $\Delta fT = 1$. Для сравнения на тот же график нанесены рабочие характеристики оптимального обнаружителя полностью известного сигнала и сигнала с флуктуирующей амплитудой и случайной начальной фазой [4].

Как видно, при очень малых отношениях сигнал/шум, оптимальный энергетический обнаружитель может оказаться чуть-чуть лучше оптимального по тому же критерию обнаружителя для полностью известного сигнала. Этот парадоксальный факт можно объяснить тем, что при равенстве мощностей случайного и детерминированного (полностью известного приемнику) сигналов, случайный с большой вероятностью будет превосходить по уровню амплитуду детерминированного сигнала. Это видно из сравнения плотностей распределения процессов на входе порогового устройства (нормального при полностью известном сигнале и χ^2 при энергетическом обнаружении). Кстати, тот же эффект наблюдается при сравнении рабочих характеристиках обнаружителей полностью известного сигнала и сигнала со случайной федингующей амплитудой.

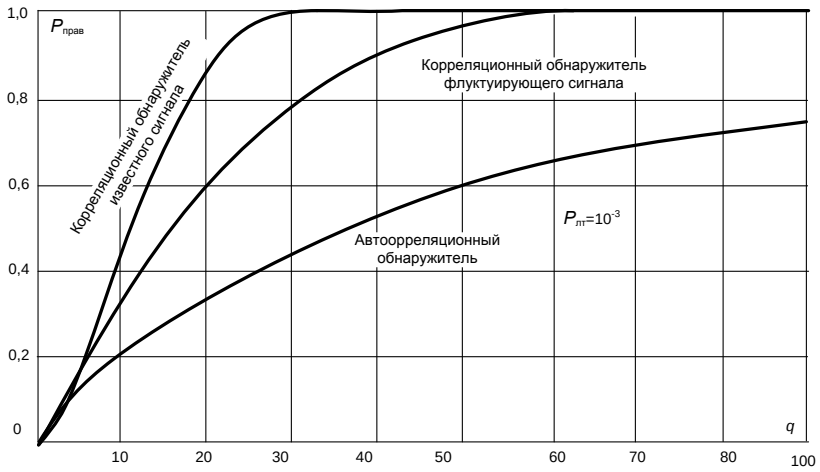


Рис. 5. Рабочие характеристики согласованного и энергетического обнаружителей

На рис. 6. изображены рабочие характеристики энергетического обнаружителя при разных уровнях вероятностей ложных тревог. Соответственно, сверху-вниз $P_{лт} = 10^{-1}$; 10^{-2}; 10^{-3} и 10^{-4}.

Число степеней свободы (параметр накопления $B = \Delta fT$) всюду на рис. 6 принят равным $B = 1$.

Увеличение значения параметра накопления повышает крутизну рабочих характеристик оптимального энергетического обнаружителя. Этот эффект иллюстрируется семейством кривых на рис. 7.

3. Оценка энергетической скрытности

Иногда удобнее сравнивать качество работы обнаружителей сигнала не по вероятностям их ошибок, а по пороговым уровням мощностей сигналов, обнаруживаемых с заданными вероятностями. Для примера на рис. 8 приведены семейства зависимости проигрыша по энергетике энергетического рис. 2 обнаружителя обнаружителю полностью известного сигнала. На этом рисунке K – превышение соотношения сигнал/шум $q_{эн}$ для энергетического обнаружителя над соответствующим соотношением для корреляционного обнаружителя полностью известного сигнала $q_к$, при условии, что оба этих обнаружителя обеспечивают одинаковые вероятности ошибок. Семейство кривых на рис. 8 *a*) получено для значения параметра накопления $\Delta fT = 1$; 2 и 5. Как видно, различие оптимального и энергетического обнаружителей резко усугубляется с ростом требований к вероятности правильного обнаружения. Параметром семейства кривых на рис. 8 *b*) служит значение вероятности ложной тревоги, допустимое при работе обнаружителя.

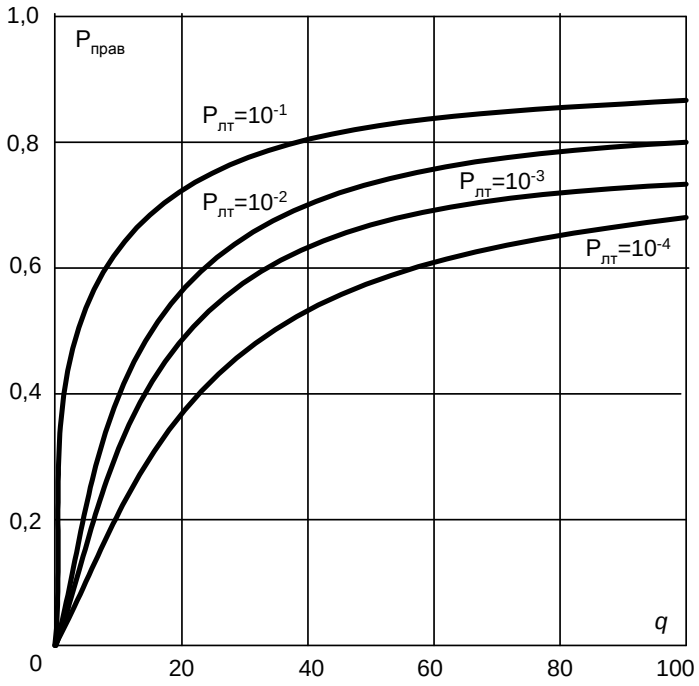


Рис. 6. Рабочие характеристики энергетического обнаружителя при $P_{лт} = 10^{-1}$, $P_{лт} = 10^{-2}$, $P_{лт} = 10^{-3}$, $P_{лт} = 10^{-4}$

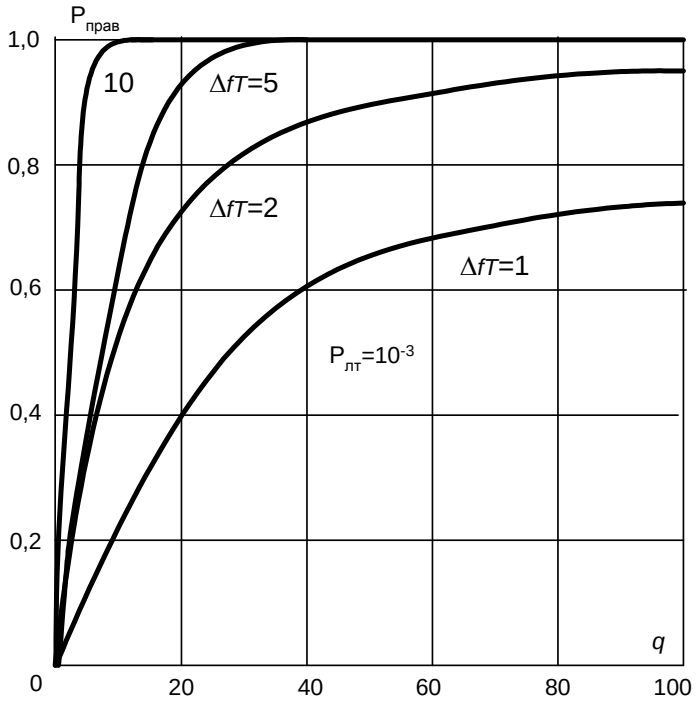
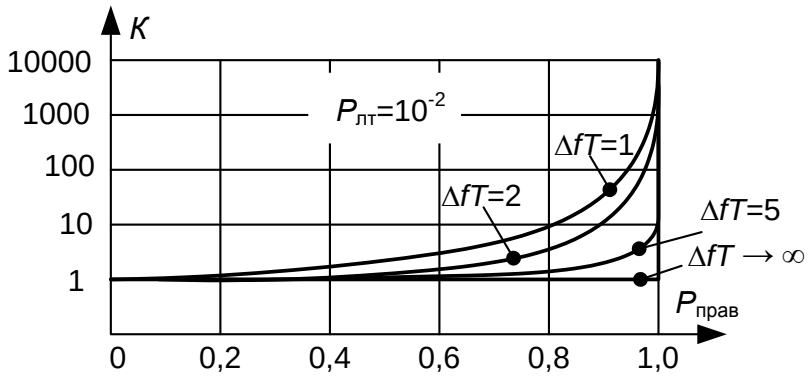
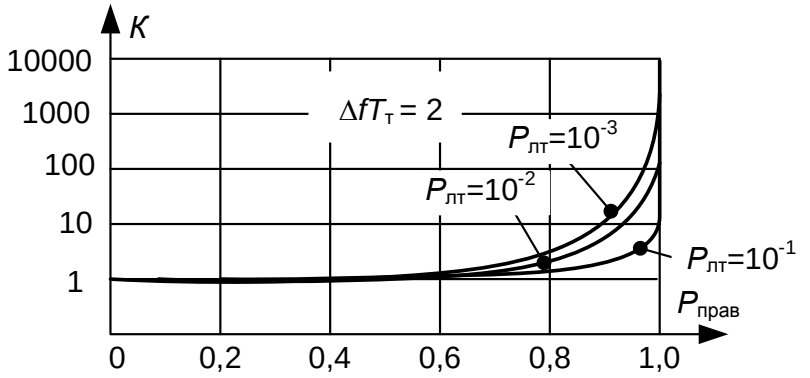


Рис. 7. Зависимости рабочих характеристик энергетического обнаружителя от числа степеней свободы процесса на входе решающего устройства – от базы $B = \Delta fT$



a)



b)

Рис. 8. Проигрыш энергетического обнаружителя оптимальному обнаружителю полностью известного сигнала

Использованное при расчете зависимостей рис. 5 условие равенства базы сигнала на входе корреляционного обнаружителя и информационной емкости процесса на входе обнаружителя энергетического $\Delta fT = \Delta f_ш T$ противоречит, вообще говоря, принятому ранее условию априорной параметрической неопределенности обнаружителя в составе средства РЭБ. Поэтому следует уточнить возможные соотношения между шириной спектра сигнала Δf и полосой анализа приемника разведки, обеспечивающего оперативную поддержку работы средства РЭБ.

1) Широкополосный сигнал $\Delta f >> \Delta f_ш$.

При этом спектр сигнала распределен между $n \approx \Delta f/\Delta f_ш$ параллельно работающими энергетическими обнаружителями и соотношение сигнал/шум в полосе каждого примерно в n раз меньше, чем в полосе Δf. Соответственно меньше будет и вероятность правильного обнаружения, влияющая на вероятность постановки прицельной по частоте помехи. Этим эффектом обычно объясняется энергетическая скрытность сигнала, обеспечиваемая за счет расширения его спектра.

2) Очень узкополосный сигнал $\Delta f << \Delta f_ш$.

Спектр сигнала с большой вероятностью сосредоточен во входной полосе $\Delta f_ш$ одного обнаружителя и надежно обнаруживается. Для обеспечения энергетической скрытности может быть применен иной метод расширения спектра, а именно – псевдослучайная перестройка частоты, когда каждый следующий информационный символ излучается на иной частоте.

При ППРЧ каждый символ (или даже часть символа) длительностью $\tau \sim 1/\Delta f$ может работать на одной из N сменных несущих частот f_i, $i \in 1, \ldots, N$. Приемник средства РРТР

разведки обнаруживает сигнал с вероятностью, оцененной соотношением (9) и настраивает постановщик помех на те же несущие частоты f_{pj}, выбранные из того же множества мощностью N. Не будет преувеличением считать, что все эти частоты известны средству радиотехнической разведки по накопленным за длительное время данным. В условиях применения скачков частоты эффективность разведки и, соответственно, скрытность от нее, будет характеризоваться уже не вероятностью $P_{\text{прав}}$, а некоторой другой величиной

$$P'_{i,j} = P_{i,j} P_{\text{прав}}, \tag{10}$$

где P_{ij} – вероятность того, что приемник разведки настроен на j-ю рабочую РЭС частоту передатчика, тогда как передатчик работает на частоте f_{ci}.

Если приемник радиотехнической разведки угадал несущую частоту сигнала и настроился на эту частоту, он обеспечит подавление обнаружения сигнала РЭС с вероятностью P_{ii}. Если не угадал, эффективность обнаружения будет ниже, а скрытность, соответственно, выше: $P_{ij} \geq P_{ii}$ для всех $i \neq j$. Очевидно, усредненное по множеству всех возможных ситуаций, складывающихся в конфликте средств радиоэлектронной разведки и радиозащиты РЭС, значение показателя эффективности маскировки будет

$$\langle P \rangle = P_{ii} \frac{1}{N} + P_{ij} \frac{N-1}{N} \to P_{ij} \text{ при } N \to \infty. \tag{11}$$

Если только $P_{ij} > P_{ii}$, а это условие обязательно должно выполняться для любой рациональной стратегии обеспечения скрытности. Из (11) следует, что $\langle P \rangle$ увеличивается с ростом числа рабочих частот N и стремится к P_{ij}. Иначе говоря, при использовании для маскировки скачков по частоте, скрытность РЭС растет как с ростом числа рабочих частот N, так и с увеличением $P_{\text{прав}}$.

Выводы

Таким образом, по результатам рассмотрения условий работы обнаружителя сигнала в составе аппаратуры средства радиоэлектронной разведки можно сделать следующие выводы.

1) Традиционно рассматриваемые модели параметрической неопределенности сигнала, маскируемого от средств радио- и радиотехнической разведки, должны быть дополнены моделями, учитывающими особенности работы энергетического (автокорреляционного обнаружителя) в составе средств РРТР.

2) Расширение спектра сигнала (точнее – увеличение его базы $B = \Delta f T$) улучшает скрытность от средств разведки. Но уменьшение полосы спектра информационного сигнала Δf, ухудшающее скрытность, может быть скомпенсировано применением псевдослучайной перестройки несущей частоты от символа к символу, или даже чаще.

3) Сама возможность постановки помехи, прицельной по частоте сигнала, обусловлена надежностью измерения этой частоты, т. е. вероятностью обнаружения сигнала в полосе анализирующего фильтра приемника РРТР. Поэтому защита от такой помехи должна предусматривать меры противодействия разведки. Среди таких мер необходимо рассматривать и исследовать способы, основанные на дезинформации разведывательного приемника.

Литература

1. Ширман Я.Д. Радиоэлектронные системы: основы построения и теория – М.: ЗАО «Максвис», 1998. – 828 с.

2. Янке Е., Эмде Ф., Леш Ф. Специальные функции. – М.: Наука, 1968. – 344 с.

3. Куприянов А.И., Шустов Л.Н. Радиоэлектронная борьба. Основы теории. – М.: Вузовская книга, 2011. – 800 с.

4. Тихонов В.И. Статистическая радиотехника. – М.: Сов. радио, 1966. – 678 с.

References

1. Shirman Ya.D. *Radioelektronnye sistemy: osnovy postroeniya i teoriya* [Radio-electronic systems: fundamentals of the construction and theory]. Moscow, CJSC "Maksvis", 1998. 828 p. (in Russian).

2. Yanke E., Emde F., Lesh F. *Special'nye funkcii* [Special functions]. Moscow, Science Publ., 1968. 344 p. (in Russian).

3. Kupriyanov A.I., Shustov L.N. *Radioelektronnaya bor'ba. Osnovy teorii* [Electronic warfare. Fundamentals of theory]. Moscow, University book Publ., 2011. 800 p. (in Russian).

4. Tikhonov V.I. *Statisticheskaya radiotekhnika* [Statistical radio engineering]. Moscow., Soviet radio Publ., 1966. 678 p. (in Russian).

Статья поступила 24 мая 2021 г.

Информация об авторе

Куприянов Александр Ильич – Доктор технических наук, профессор. Профессор Московского авиационного института (национального исследовательского университета). Адрес: 125993, Москва, Волоколамское шоссе, д. 4, А-80, ГСП-3. Тел.: +7-910-469-09-55. E-mail: kupriyanovai@mai.ru.

The secrecy of super-narrowband signals

A.I. Kupriyanov

Annotation. *The article considers the operating conditions of a signal detector as part of a radio-electronic device. At the same time, the spectrum of the analyzed signal is estimated according to the quality indicators of its detection against a noise background due to both the receiver's own noise and the external noise field. The structure of an autocorrelation (energy) detector of an a priori unknown signal is presented. Graphs of the probability distribution density of the squares of the input normal process for various accumulation parameters are constructed. A diagram of the exchange between errors of the first and second kind in the energy detection of a signal is given. The operating characteristics of the matched and energy detectors at different levels of false alarm probabilities are determined. The value of the loss of the energy detector to the optimal detector of a previously known signal is calculated. As a result of the study, it is shown that the expansion of the signal spectrum improves stealth from intelligence means. However, the decrease in the spectrum band of the information signal, which worsens the secrecy, can be compensated by the use of pseudo-random tuning of the carrier frequency from symbol to symbol, or even more often. The very possibility of interference, aimed at the signal frequency, is due to the reliability of measuring this frequency. Therefore, protection against such interference should include counter-intelligence measures. Among such measures, it is necessary to consider and investigate methods based on the disinformation of the intelligence receiver.*

Keywords: *optimal energy signal detector, accumulation parameter, decision device, radio signal stealth, broadband signal.*

Информация об авторе

Kupriyanov Alexander Ilyich – Doctor of Technical Sciences, Professor. Professor of the Moscow Aviation Institute (National Research University). Address: 125993, Moscow, Volokolamsk highway, 4, A-80, GSP-3. Tel. +7-910-469-09-55. E-mail: kupriyanovai@mai.ru.

Для цитирования: Куприянов А.И. Скрытность сверхузкополосных сигналов // Техника средств связи. 2021. № 2 (154). С. 2-11.

For citation: Kupriyanov A.I. The secrecy of super-narrowband signals. Means of communication equipment. 2021. No 2 (154). Pp. 2-11 (in Russian).

СИСТЕМЫ СВЯЗИ И ТЕЛЕКОММУНИКАЦИИ

УДК 621.396.93

Пространственные параметры линии метеорной радиосвязи

Комашинский В.И., Кулешов И.А., Солозобов С.А., Щукин А.Н.

Аннотация. *Цель статьи – показать, как с использованием данных, полученных от глобальной системы навигации «ГЛОНАС», можно улучшить точность ориентации антенн станций метеорной радиосвязи при планировании их развертывания. Большой научный интерес представляет вопрос, в какую точку небесного пространства должны быть ориентированы диаграммы направленности передающей и приемной антенн линии метеорной радиосвязи. Теоретический анализ показывает, что наилучшие результаты достигаются при некотором отклонении диаграмм направленности обеих антенн в сторону от направления основной трассы. Приведена структура линии метеорной радиосвязи, реализующая возможность использования параметров, определяемых глобальной системой навигации, для планирования развертывания станций метеорной радиосвязи. Представлены результаты расчета в геодезической системе координат пространственных параметров для линии метеорной радиосвязи, показывающие величину отклонения диаграмм направленности антенн от направления по основной оси трассы. Выполнен анализ результатов расчета азимутов и углов места для трассы, развертываемой вдоль параллели северного полушария Земли. Результаты работы могут быть реализованы при построении линий и сетей метеорной радиосвязи.*

Ключевые слова*: линия метеорной радиосвязи, геодезическая система, азимут, угол места, точка отражения, отклонение диаграмм направленности антенн.*

Введение

Характерным для линий метеорной радиосвязи (МРС) является образование ионизированных метеорных следов, создаваемых метеорными частицами, вторгающимися в атмосферу Земли со скоростями в несколько десятков километров в секунду, и сталкиваясь с молекулами и атомами разряженного воздуха. Высота ионизированных слоев – от 80 до 120 километров.

Электромагнитные волны отражаются от ионизированных метеорных следов, для которых объемная электронная плотность удовлетворяет условию

$$N > \lambda^2/81, \quad (1)$$

где: N – объемная электронная плотность, электрон/м^3; λ – длина волны частоты излучения, м.

Средняя длина ионизированного следа составляет, примерно 25 км.

Возможности современной глобальной системы навигации «ГЛОНАС» позволяют использовать её данные для более точного, чем ранее, определения пространственных параметров (азимута и угла места) линий МРС и прецизионного наведения диаграмм направленности (ДН) приемной и передающей антенн, что открывает возможности по существенному повышению эффективности функционирования линий и сетей метеорной радиосвязи.

1. Определение средней точки линии метеорной радиосвязи

При определении пространственных параметров линии МРС в качестве системы координат, для определения точек на земной поверхности и в околоземном пространстве, будем использовать геодезическую систему координат (прямоугольную (x, y, z) и криволинейную (B, L, H).

Положение точки в пространстве задается геодезическими криволинейными *B*, *L*, *H* или геодезическими прямоугольными (декартовыми) координатами *x*, *y*, *z*. Связь между ними задается формулами [1]:

$$x = (N+H)\cos(B)\cos(L),$$
$$y = (N+H)\cos(B)\sin(L), \quad (2)$$
$$z = (N(1-e^2)+H)\sin(B).$$

где: *B* – геодезическая широта объекта; *L* – геодезическая долгота объекта; *H* – геодезическая высота объекта; e – эксцентриситет эллипсоида; *N* – радиус кривизны первого вертикала; *x*, *y*, *z* – геодезические прямоугольные координаты.

Обратный переход к геодезическим криволинейным координатам, с приемлемой для определения пространственных параметров линии МРС точностью, задается формулами

$$B = \text{arctg}\,(z/D\,(1+e^2a/R\sqrt{1-e^2}),$$
$$L = \text{arctg}\,(y/x), \quad (3)$$

где: $D = \sqrt{x^2+y^2}$; $R = \sqrt{x^2+y^2+z^2}$; a – большая полуось эллипсоида.

Пусть заданы геодезические координаты двух станций МРС в виде:

С.Ш. корреспондента «А» – [59° 46′ 15″]; В.Д. – [30° 19′ 28″];

С.Ш. корреспондента «В» – [65° 51′ 25″]; В.Д. – [74° 21′ 03″].

Преобразуем эти координаты в десятичную форму представления геодезических координат

$$a^\circ\, b'\, c'' = (a+b/60+c/3600)^\circ.$$

С использованием выражения (2) определим координаты корреспондентов в прямоугольной геодезической системе координатам.

Представим эти координаты в векторной форме, как

$\overrightarrow{vA}$ = [xA, yA, zA] – корреспондент «А»,

$\overrightarrow{vB}$=[xB, yB, zB] – корреспондент «В».

Определим среднюю точку (область пересечения ДН антенн станций МРС) трассы и ее координаты (*B*3, *L*3) на поверхности Земли

$$\overrightarrow{mid} = \overrightarrow{vA} + \overrightarrow{vB},$$
$$B3 = \text{arctg}(\text{mid}(3)/\sqrt{(\text{mid2}(1)+\text{mid2}(2))}), \quad (4)$$
$$L3 = \text{arctg}(\text{mid}(2)/\text{mid}(1)).$$

В скобках указаны элементы вектора $\overrightarrow{mid}$.

С использованием выражения (2) и с учетом выражения (4) определим координаты точки на высоте существования метеорных следов *HP*

$$xP = (N+HP)\cos(B3)\cos(L3),$$
$$yP = (N+HP)\cos(B3)\sin(L3), \quad (5)$$
$$zP = (N(1-e^2)+HP)\sin(B3).$$

На рис. 1 представлена структура линии МРС с координатами точки отражения $B3 \rightarrow X = 64{,}94^\circ$ С.Ш., $L3 \rightarrow Y = 50{,}64^\circ$ В.Д., $HP \rightarrow Z = 90$ км.

2. Определение азимута на корреспондента и точки отражения

Определим азимуты от корреспондента «А» на корреспондента «В» и обратно, по формулам, приведенным в [2]

$$azAB = \text{arctg}\,(B2-B1/q2-q1), \quad (6)$$
$$azBA = azAB+\pi,$$

где: $q = \ln\{\text{arctg}(\pi/4+B/2)\sqrt{\left(\frac{1-e\sin(B)}{1+e\sin(B)}\right)^{e/2}}\}$ – изометрическая широта; $B = B1$ или $B2$ или $B3$.

Теперь определим азимуты от корреспондентов «А» и «В» на точку отражения

$$az13 = \text{arctg}\,(B3 - B1/q3 - q1), \quad (7)$$

$$az23 = \text{arctg}\,(B3 - B2/q3 - q2). \quad (8)$$

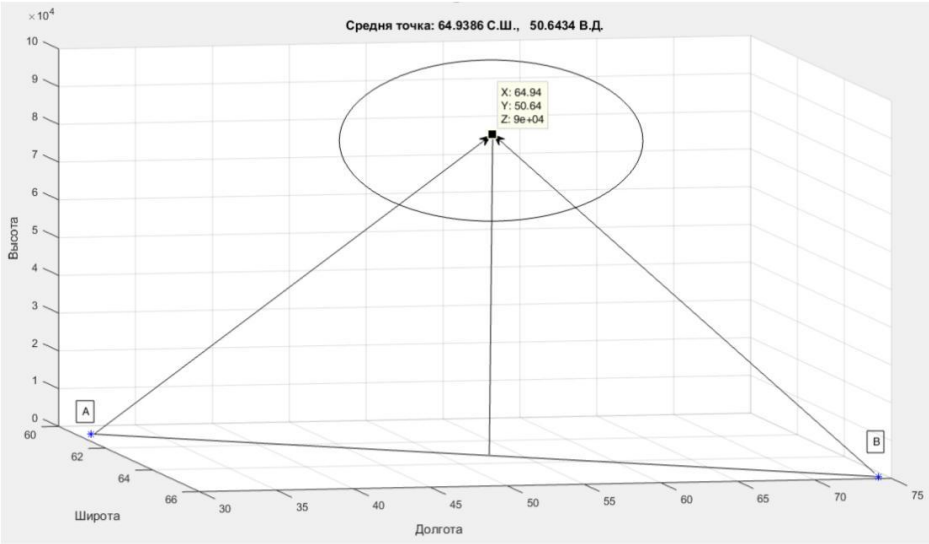


Рис. 1. Структура линии МРС

Результаты расчета по формулам (6), (7), (8), проведенные для нескольких пар координат, представлены на графиках рис. 2.

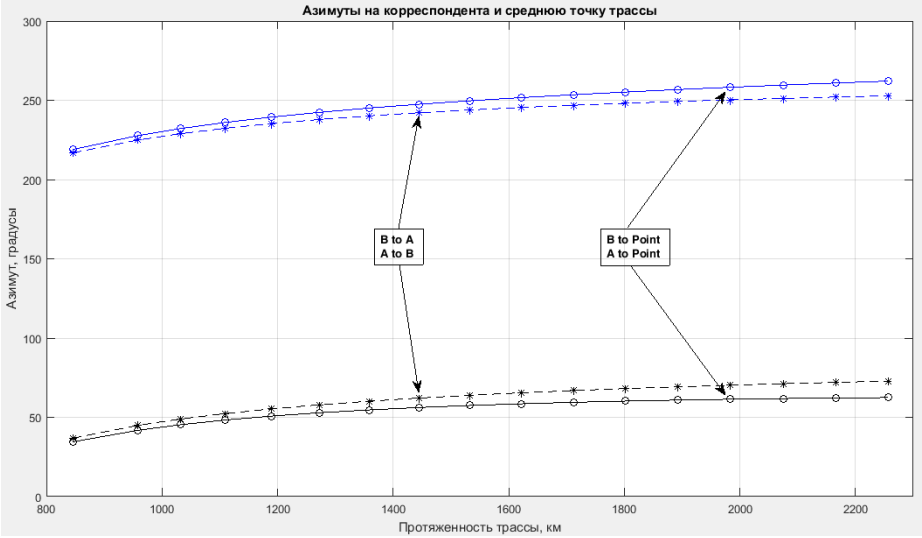


Рис. 2. Азимуты на корреспондентов и точку отражения от метеорных следов

Из рис. 2 видно, что линии от корреспондентов на точку отражения луча (*B to Point* и *A to Point*) отличаются от графиков на корреспондентов друг на друга (*B to A* и *A to B*). Причем, с увеличением протяженности, трассы различия увеличиваются.

Определяя угол расхождения между прямым и обратным азимутами и азимутами на точку отражения от корреспондентов, и используя выражение [3], определим, сколько километров составляет один градус угла отклонения азимутов (*B to Point* и *A to Point*) и (*B to A* и *A to B*) на различных удалениях корреспондентов от точки отражения.

$$S^{o} = 2dst(A,B)\ pi/360, \quad (9)$$

где: *dst(A, B)* – расстояние от корреспондентов «А» или «В» до точки отражения, км.

Определим разницу азимутов на корреспондентов и точку отражения

$$azA3 = azAB - az13, \quad (10)$$

$$azB3 = az23 - azBA. \quad (11)$$

Определим расхождение лучей в точке отражения как

$$otklA = dstA * azA3, \quad (12)$$

$$otklB = dstB * azB3. \quad (13)$$

Результаты расчета расхождение лучей в точке отражения по формулам (12), (13) представлены на рис. 3.

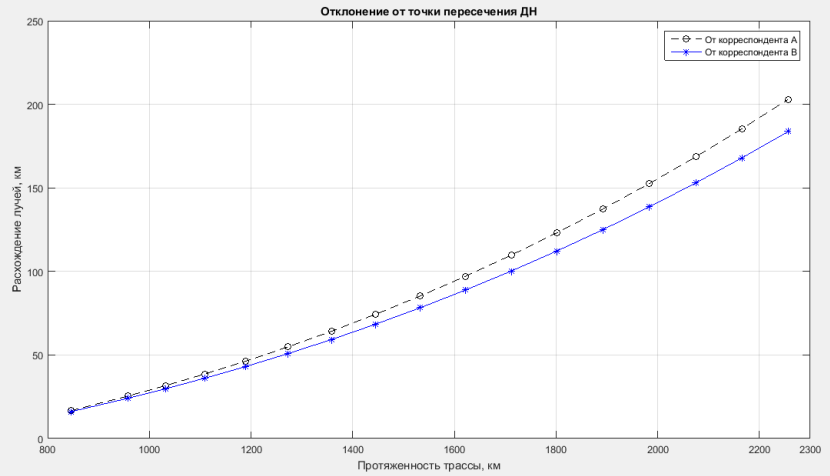


Рис. 3. Расхождение лучей ДН антенн в точке отражения

Из рис. 3 видно, что расхождение лучей ДН антенн как от корреспондента «А», так и корреспондента «В», составляет от нескольких десятков километров до двух сотен километров для трасс большой протяженности. Это указывает на то, что часть метеорных следов не попадают в область пересечения ДН антенн, и, следовательно, не используются для отражения электромагнитных волн.

3. Определение угла места на точку отражения

Расчет угла места корреспондентов «А» и «В» на точку отражения осуществляется путем определения угла между векторами в направлении на корреспондента «А» или «В» и точку отражения с использованием выражений (для корреспондента «А» (Θ_{AP}) и корреспондента «В» (Θ_{BP})) [4]

$$\Theta_{AP} = \arccos\left(\frac{|\overrightarrow{vAp} * \overrightarrow{vAB}|}{|\overrightarrow{vAp}| * |\overrightarrow{vAB}|}\right), \quad (14)$$

$$\Theta_{BP} = \arccos\left(\frac{|\overrightarrow{vBp} * \overrightarrow{vBA}|}{|\overrightarrow{vBp}| * |\overrightarrow{vBA}|}\right), \quad (15)$$

где: $\overrightarrow{vAp}$ =[xP-x1, yP-y1, zP-z1] – длина вектора в точку отражения от корреспондента «А»;

$\overrightarrow{vBp}$ = [xP-x2, yP-y2, zP-z2] – длина вектора в точку отражения от корреспондента «В»;

$\overrightarrow{vBA}$ =[x2-x1, y2-y1, z2-z1] – длина вектора в направлении корреспондента «А»;

$\overrightarrow{vAB}$ = [x1-x2, y1-y2, z1-z2] – длина вектора в направлении корреспондента «В».

Результаты расчета расхождение лучей в точке отражения по формулам (14), (15) представлены на рис. 4.

Из рис. 4 видно, что с увеличением протяженности трассы МРС угол места уменьшается и на дальности около 2200 километров составляет около 9.5^{o}. Небольшое отличие в углах места корреспондентов на точку отражения обусловлена отличием высот размещения станций МРС и кривизной Земли.

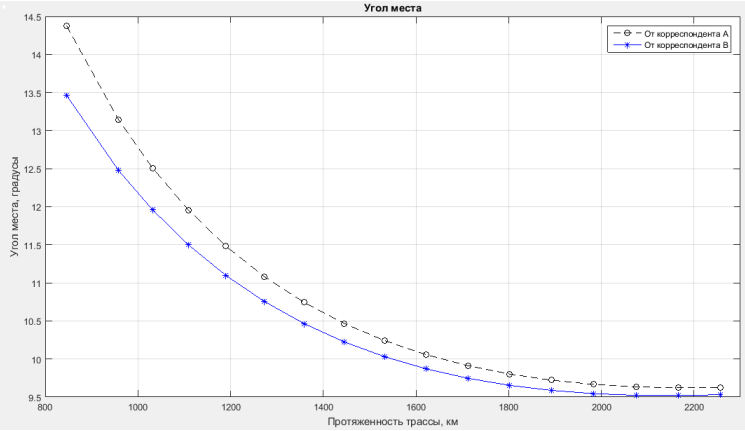


Рис. 4. Угол места точки отражения от корреспондентов «А» и «В»

Таким образом, для функционирования станций МРС необходимо, помимо назначения для нее частотно-энергетических параметров, провести расчет азимутов корреспондентов на точку отражения и углов места от них на точку отражения.

Для определения пространственных параметров линий МРС необходимо:

1) Определить координаты середины трассы МРС.
2) Преобразовать эти координаты к высоте появления отражающих метеорных следов.
3) Определить азимуты от корреспондентов на точку отражения.
4) Определить углы места от корреспондентов на точку отражения.

Выводы

Для построения линий и сетей МРС важную роль играют данные, полученные от глобальной системы навигации «ГЛОНАС».

Полученные в работе результаты открывают новые перспективы построения более эффективных чем ранее, линий и сетей МРС.

Для целенаправленного выбора точек пересечения ДН антенн целесообразно провести исследования по определению областей наиболее интенсивного появления метеорных следов с высокой объемной электронной плотностью.

Литература

1. Бойко Е.Г. Высшая геодезия. Часть 11. Сфероидическая геодезия: учебник для вузов. –М.: Картгеоцентр – Геодезиздат, 2003. – 144 с.

2. Утешева Т.Ш. Математическое проецирование в ГИС: учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2016. – 60 с.

3. Клепко В.Л., Александров А.В. Системы координат в геодезии: монография. – Екатеринбург: Уральский государственный горный университет, 2011. – 116 с.

4. Айдаркин Д.В. Векторная алгебра и метод координат: Учебное пособие. – Ульяновск: УВАУГА, 2007. – 116 с.

References

1. Boyko E.G. Higher geodesy. Part 11. Spheroidal geodesy. Textbook for universities. Moscow. Kartgeocenter-Geodesizdat. 2003. 144 p. (in Russian).

2. Utesheva T.S. Mathematical projection in GIS: an educational and methodological guide. Nizhny Novgorod. Nizhny Novgorod State University. 2016. 60 p. (in Russian).

3. Klepko V.L., Alexandrov A.V. Coordinate systems in geodesy: A scientific monograph. Yekaterinburg. Ural State Mining University. 2011. 116 p. (in Russian).

4. Aidarkin D.V. Vector algebra and the coordinate method: A textbook. Ulyanovsk. UVAUGA. 2007. 116 p. (in Russian).

Статья поступила 02 июня 2021 г.

Информация об авторах

Комашинский Владимир Ильич – Доктор технических наук, доцент, заместитель директора по научной работе. Институт проблем транспорта им. Н.С. Соломенко РАН. Адрес: Санкт-Петербург, В.О.,12 линия, д.13. E-mail: kama54@rambler.ru, тел.: (812)323-29-54.

Кулешов Игорь Александрович – Доктор технических наук, доцент, заместитель генерального директора по научной работе, ПАО «Интелтех». Адрес: Санкт-Петербург, ул. Кантемировская, д. 8. E-mail: KuleshovIA@inteltech.ru, тел.: (812)542-90-54.

Солозобов Сергей Анатольевич – Кандидат технических наук, доцент, начальник НИО, ПАО «Интелтех». Адрес: Санкт-Петербург, ул. Кантемировская, д. 8. E-mail: solozobob@inteltech.ru, тел.: (812)295-40-54.

Щукин Анатолий Николаевич – Кандидат технических наук, главный специалист ПАО «Интелтех». Адрес: Санкт-Петербург, ул. Кантемировская д.8. E-mail: ShchukinAN@inteltech.ru, тел.: (812)448-95-94.

Spatial parameters of the meteor radio communication line

V.I. Komashinsky, I.A. Kuleshov, S.A. Solozobov, A.N. Shchukin

Annotation. *The purpose of the article is to show how using data obtained from the GLONAS global navigation system, it is possible to improve the accuracy of orientation of the antennas of meteor radio stations when planning their deployment. Of great scientific interest is the question at which point in celestial space the directional patterns of the transmitting and receiving antennas of the meteor radio link should be oriented. Theoretical analysis shows that the best results are achieved with some deviation of the directional patterns of both antennas away from the direction of the main route. The structure of the meteor radio communication line is given, which realizes the possibility of using parameters determined by the global navigation system for planning the deployment of meteor radio communication stations. Results of calculation in geodetic system of coordinates of spatial parameters for line of meteor radio communication showing value of deviation of antenna directivity patterns from direction along main axis of route are presented. Analysis of results of calculation of azimuths and angles of place for route deployed along parallel of Earth's northern hemisphere is performed. The results of the work can be implemented during the construction of meteor radio communication lines and networks.*

Keywords: *meteor radio communication line, geodetic system, azimuth, elevation angle, reflection point, deviation of antenna directional patterns.*

Information about Authors

Vladimir Ilyich Komashinsky – Doctor of Technical Sciences, Associate Professor, Deputy Director for Research, N.S. Solomenko Institute of Transport Problems of the Russian Academy of Sciences. Address: St. Petersburg, V.O., 12 liniya, 13. E-mail: kama54@rambler.ru. Tel. (812)323-29-54.

Igor Aleksandrovich Kuleshov – Doctor of Technical Sciences, Associate Professor, Deputy General Director for Research, PJSC "Inteltech". Address: St. Petersburg, Kantemirovskaya Street, 8. E-mail: KuleshovIA@inteltech.ru. Tel. (812)542-90-54.

Sergey Anatolyevich Solozobov – Candidate of Technical Sciences, Associate Professor, Head of NIO-0630, PJSC "Inteltech". Address: St. Petersburg, Kantemirovskaya street, 8. Tel. (812)295-40-54. E-mail: solozobob@inteltech.ru.

Anatoly Nikolaevich Shchukin – Candidate of Technical Sciences, Chief Specialist of PJSC "Inteltech". Address: St. Petersburg, Kantemirovskaya Street, 8. E-mail: ShchukinAN@inteltech.ru. Tel. (812)448-95-94.

Для цитирования: Комашинский В.И., Кулешов И.А., Солозобов С.А., Щукин А.Н. Пространственные параметры линии метеорной радиосвязи // Техника средств связи. 2021. № 2 (154). С. 12-17.

For citation: Komashinsky V.I., Kuleshov I.A., Solozobov S.A., Shchukin A.N. Spatial parameters of the meteor radio communication line. Means of Communication Equipment. 2021. No. 2 (154). Pp. 12-17 (in Russian).

УДК 004.72

Алгоритм сопряжения гетерогенных сетей передачи данных

Кулешов И.А., Мержеевский А.А.

Аннотация: *Целью работы является определение рационального алгоритма сопряжения гетерогенных сетей передачи данных, в которых применяются различные стеки сетевых протоколов, с учетом существующих проблем их взаимодействия. В работе приводится алгоритм сопряжения двух и более гетерогенных сетей с использованием внешних шлюзов. Отмечены достоинства и недостатки сопряжения сетей с применением централизованного внешнего шлюза и распределенного внешнего шлюза. Результатом работы является обобщенный алгоритм сопряжения гетерогенных сетей передачи данных с использованием протокола межсетевого взаимодействия и распределенных внешних шлюзов. Практическая значимость работы направлена на определение способов применения существующих и разработки новых методов объединения гетерогенных сетей передачи данных специального назначения.*

Ключевые слова: *гетерогенная сеть передачи данных, алгоритм сопряжения, внешний шлюз, межсетевой протокол.*

Введение

В последние годы в Вооруженных Силах Российской Федерации (ВС РФ) ведется активное внедрение новых систем связи и управления. Разработаны и строятся современные автоматизированные системы управления (АСУ). Практика создания автоматизированных систем специального назначения показала сложность решения задачи их увязки в единую автоматизированную систему управления Вооруженных Сил. В ходе выполнения предприятиями оборонно-промышленного комплекса работ по автоматизации управления ВС РФ сложилось положение, при котором существующие и разрабатываемые автоматизированные системы военного назначения слабо совместимы или несовместимы [1].

В РФ для обеспечения функционирования более 270 специализированных АСУ используют более 20 типов транспортных сетей связи и более 70 типов сетей доступа специального назначения различных ведомств. Всего в этом случае возможно более 7 млн вариантов построения сетей связи для обеспечения выполнения требований различных специализированных систем управления [2].

Для организации взаимодействия узлов сетей связи используются многоуровневые структуры – стек протоколов. В однородной сети связи все элементы сети используют один и тот же стек. В контексте межсетевого взаимодействия понятие «сеть» можно определить как совокупность технических средств, общающихся друг с другом с помощью единого стека протоколов [3]. Стек протоколов физически реализуется с помощью программно-аппаратных средств. Согласованный набор протоколов и реализующих их программно-аппаратных средств, достаточный для построения вычислительной сети, далее по тексу будет называться – базовая сетевая технология (БСТ). Исходя из вышеизложенного, можно сделать вывод, что в однородной сети связи используется единая базовая сетевая технология, которая обеспечивает доведение передаваемой информации от отправителя до получателя в рамках «своей» сети.

Согласно [4], современные системы связи специального назначения (СС СН) и их перспективы развития имеют следующие основные тенденции по технологическому построению:

переход от иерархического принципа построения СС СН, когда ее структура жестко увязывается со структурой организационной подчиненности абонентов к децентрализованной сетевой структуре, которая не зависит от организации системы подчиненности абонентов, и в большей степени соответствует современным требованиям к сетецентрическим системам государственного и военного управления;

отказ от построения СС СН на основе отдельной связной инфраструктуры и переход к построению СС СН на основе гибридного подхода, когда отдельные сегменты СС общего пользования национальных и региональных операторов связи, а также сегменты глобальных сетей используются в качестве элементов транспортной инфраструктуры СС СН;

максимальное широкое использование для построения СС СН подходов, протоколов и технологий, применяемых в гражданской сфере связи и телекоммуникаций.

Данные тенденции технологического построения СС СН приводят к необходимости использования различных стеков протоколов для организации взаимодействия элементов СС СН, что ведет к росту неоднородности сети в целом. Под неоднородностью (гетерогенностью) сети понимают несовместимость двух узлов, принадлежащей одной сети, либо к смежным сегментам сети по одному или нескольким логическим признакам: форматам кадров сети; типу применяемых операционных систем; способам защиты информации; применимым моделям безопасности и пр. [5].

В настоящее время существует три основных метода сопряжения гетерогенных сетей связи (ГСС): трансляции; мультиплексирования; инкапсуляции.

Метод трансляция описан как способ согласования двух протоколов ГСС путем преобразования (трансляции) сообщений, поступающих от одной сети, в формат другой сети. Метод мультиплексирования ГСС состоит в установке нескольких дополнительных стеков протоколов на одном из конечных устройств, участвующих во взаимодействии. Метод инкапсуляции ГСС по результатам анализа заключается в том, что подключают объединяемые сети к транзитной, которая упаковывает пакеты транспортного протокола объединяемых сетей в пакеты транспортного протокола транзитной сети [1]. Однако, в прямой постановке вопроса выбор конкретного метода сопряжения весьма затруднителен, учитывая, что гетерогенность сетей может достигать полного несоответствия протоколов всех уровней модели *OSI*. Именно такой вариант сопряжения сетей передачи данных и рассматривается в данной статье.

1. Вариант сопряжения двух гетерогенных сетей связи

Примером двух ГСС, использующих полностью различные протоколы сетевого взаимодействия, являются базовая система обмена данными АСУ ВС РФ, построенная на основе единого сетевого (стека) протокола информационного обмена (ЕСПИО), и сеть закрытого сегмента передачи данных, построенная на базе стека протоколов *TCP/IP*.

Согласно [6] протоколы делятся на сетезависимые и сетенезависимые. К сетезависимым протоколам относятся протоколы нижних уровней модели *OSI* – физического, канального, сетевого и транспортного, к сетенезависимым относиться протоколы верхних уровней модели *OSI* – сеансового, представительского и прикладного. Так как в настоящей статье речь идет о сетевом взаимодействии, то согласование протоколов верхних уровней остаётся вне поля данной работы, и основное внимание уделено взаимодействию и согласованию сетезависимых протоколов нижних уровней, для которых информация, поступившая от верхних уровней является данными, которые необходимо передать от отправителя к получателю, и которые могут быть «закрыты» специализированной шифровальной аппаратурой связи (ШАС).

Помимо несоответствия методов физической передачи сигналов, структуры данных и кодировок передаваемых сообщений, основная проблема взаимодействия ГСС заключается в несоответствии форматов и структур адресной информации сетевого уровня – адреса отправителя и получателя сообщений. Как следствие, передать информацию об адресе получателя, находящегося во взаимодействующей ГСС, с помощью БСТ сети-отправителя не представляется возможным. Информация о получателе сообщения находится в протоколах верхних уровней, доступ к которой для протоколов телекоммуникационных уровней не является целесообразным с точки зрения конфиденциальности и безопасности передаваемых данных. Трансляция сетевых адресов затруднительна и возможна только при

административном назначении узлам сети-получателя виртуальных адресов сети-отправителя сообщений и наоборот. В таком случае возможно организовать таблицу соответствия адресного пространства и производить трансляцию сетевого адреса сети-отправителя в сетевой адрес сети-получателя сообщений.

Включение дополнительного сетевого протокола к существующим БСТ взаимодействующих ГСС позволит обеспечить наиболее гибкое и рациональное сопряжение ГСС. Дополнительный протокол – «протокол межсетевого взаимодействия», предназначен для передачи адресной информации взаимодействующих ГСС с помощью соответствующих БСТ. Данный протокол должен быть «пограничным» между сетенезависимыми протоколами верхних уровней и протоколами БСТ. Для протоколов верхних уровней он должен представляться как телекоммуникационный протокол, а для телекоммуникационных протоколов его информация в виде дополнительного заголовка должна быть включена в поле данных, которые необходимо доставить от отправителя к получателю. Основная задача дополнительного протокола межсетевого взаимодействия заключается в том, чтобы доставить адресную информацию о получателе и отправителе сообщений (формат и структура адресной информации должна соответствовать форматам взаимодействующих ГСС) до оборудования, обеспечивающего информационно-логическое сопряжение ГСС.

В результате, к передаваемым данным от протоколов верхних уровней, перед тем как их передать для доставки получателю с помощью телекоммуникационных протоколов БСТ, должен быть добавлен ещё один служебный заголовок, в котором будут указаны действительные адреса отправителя и получателя пакета данных в существующем формате их сетей передачи данных, рис. 1.

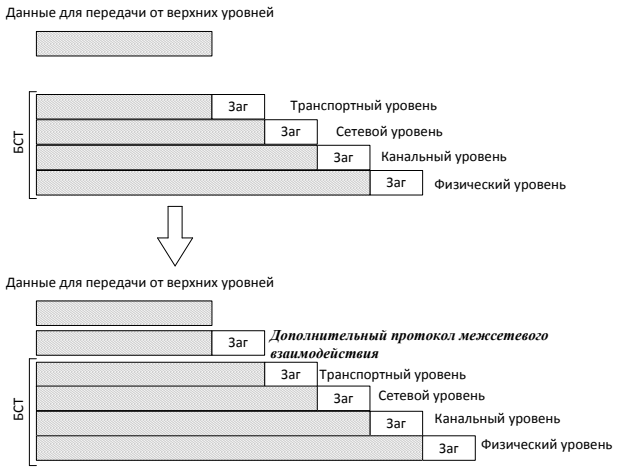


Рис. 1. Место дополнительного протокола межсетевого взаимодействия в стеке протоколов сопрягаемых сетей связи

2. Алгоритм передачи данных между узлами гетерогенных сетей связи

Учитывая, что стеки протоколов взаимодействующих ГСС различны, то для сопряжения таких ГСС предлагается использовать специализированное оборудование – внешний шлюз. Внешний шлюз должен обеспечивать поддержку БСТ и одной сети, и другой, а также обеспечивать передачу данных между данными БСТ. Техническая реализация внешнего шлюза может быть различной, начиная от специализированного изделия, реализующего всё на аппаратном уровне, и заканчивая установкой двух абонентских станций с доработанным программным обеспечением и соединённых между собой с помощью стандартного протокола передачи данных. Однако, в любом случае должны быть реализованы интерфейсы, обеспечивающие физическое сопряжение внешнего шлюза с сетью-отправителя сообщения и сетью-получателя сообщения, и на каждом из интерфейсов должно обеспечиваться функционирование протоколов БСТ соответствующих сетей.

Таким образом, каждый из интерфейсов межсетевого шлюза является полноценным абонентом сети, к которой он подключен, и доставка сообщения от отправителя до получателя в рамках данной сети осуществляется техническими средствами и протоколами сети. Передачу сообщения от узла одной ГСС до узла другой сети предлагается производить в следующей последовательности:

протоколы верхних уровней узла-отправителя формируют блоки данных, предназначенные для передачи узлу-получателю взаимодействующей ГСС, при необходимости их шифруют, и передают дополнительному протоколу межсетевого взаимодействия;

протокол межсетевого взаимодействия добавляет к полученным данным собственный заголовок, в котором указывает идентификатор сети назначения, адрес получателя в сети назначения, идентификатор собственной сети, адрес отправителя (собственный адрес), ряд дополнительных служебных полей и контрольную сумму заголовка;

полученный блок данных, включая заголовок межсетевого протокола, передаётся протоколам БСТ сети-отправителя и в качестве адреса получателя указывается сетевой адрес внешнего шлюза;

БСТ сети-отправителя доставляет блок данных до внешнего шлюза;

во внешнем шлюзе блок данных «разбирается» до уровня данных протоколов верхних уровней, из заголовка межсетевого протокола считывается идентификатор сети-назначения и адрес получателя;

блок данных, включая заголовок межсетевого протокола, передаётся протоколам БСТ сети-получателя и в качестве адреса получателя указывается сетевой адрес получателя;

БСТ сети-получателя доставляет блок данных до узла-получателя;

на узле-получателе блок данных «разбирается» до уровня данных протоколов верхних уровней и передается для обработки вышестоящим протоколам.

Вышеописанная последовательность передачи данных от узла-отправителя до узла получателя, расположенных в разных ГСС представлена схематично на рис. 2.

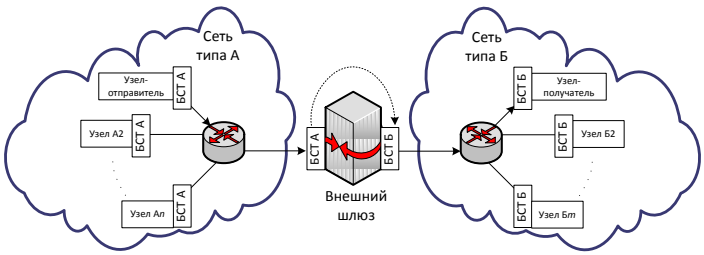


Рис. 2. Схема прохождения данных от узла-отправителя до узла-получателя, расположенных в двух ГСС

Данный алгоритм сопряжения ГСС построен на комбинированном методе мультиплексирования базовых сетевых технологий взаимодействующих сетей и трансляции сетевых адресов. При таком варианте сохраняется независимость протоколов верхних уровней от телекоммуникационных протоколов, алгоритм не нарушает действующие принципы взаимодействия телекоммуникационных протоколов и методов доставки информации в существующих сетях передачи данных и предоставляет гибкую возможность по доставки информации между гетерогенными сетями связи.

3. Сопряжение произвольного количества гетерогенных сетей связи

Для варианта с двумя ГСС вышеописанный способ сопряжения вполне пригоден и работоспособен, однако при сопряжении ГСС с использованием централизованного внешнего шлюза с ростом количества сопрягаемых ГСС резко возрастает количество вариантов преобразований передаваемой информации, происходит рост информационных потоков, проходящих через внешний шлюз, что ведет к перегруженности последнего. Зависимость количества вариантов преобразований пакетов данных от количества подключенных сетей представлена на рис. 3. В специализированных сетях передачи данных

существует ряд «закрытых» базовых сетевых технологий, доступ к которым имеет ограниченный круг пользователей, и реализация данных БСТ в одном устройстве не целесообразна с точки зрения конфиденциальности информации. В связи с этим, наиболее рациональным вариантом сопряжения произвольного количества ГСС является вариант с «распределенным шлюзом», в котором ГСС сопрягаются между собой с использованием пары внешних шлюзов и транспортной сети, обеспечивающей телекоммуникационные услуги по доставке информации, передаваемой между внешними шлюзами, рис. 4.

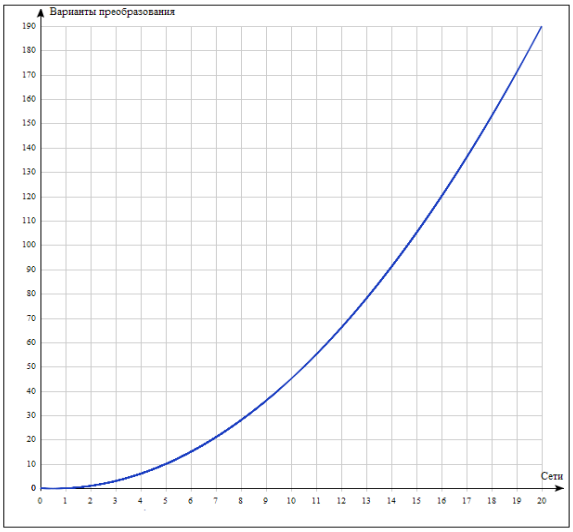


Рис. 3. Зависимость количества вариантов преобразований пакетов данных от количества подключенных сетей к шлюзу

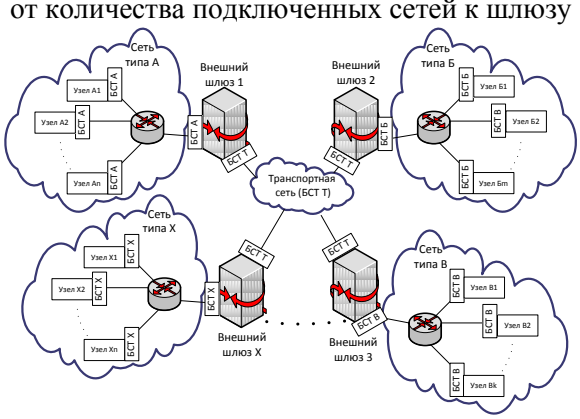


Рис. 4. Структура схема сопряжения произвольного количества ГСС с использованием двух внешних шлюзов и транспортной сети

Алгоритм сопряжения узлов, расположенных в разных ГСС с использованием двух шлюзов и транспортной сети, схож с алгоритмом, приведенным для двух ГСС. При этом на первом внешнем шлюзе отправленный блок данных передается для доставки БСТ транспортной сети и в качестве адреса получателя устанавливается сетевой адрес интерфейса второго шлюза, подключенного одновременно к транспортной сети и к сети фактического получателя блока данных. Определение сетевого адреса второго шлюза осуществляют на основе идентификатора сети-получателя, передаваемого в межсетевом заголовке блока данных. В случае использования в БСТ транспортной сети протоколов динамической маршрутизации, возможна реализация автоматического построения таблиц маршрутизации и таблиц соответствия сетевого адреса внешнего шлюза и идентификатора сети. Блок данных, доставленный БСТ транспортной сети до второго внешнего шлюза (шлюза сети получателя сообщения) с использованием алгоритма сопряжения узлов двух ГСС, определив из межсетевого заголовка адрес получателя блока данных, с помощью БСТ сети-получателя доставляет блок данных до узла-получателя.

Заключение

К широко распространенным протоколам внешней пограничной маршрутизации относятся протоколы группы *BGP* (*Border Gateway Protocol*), обеспечивающие внешнее шлюзовое взаимодействие и взаимодействие автономных систем в сети Интернет [6, 7]. Однако, данные протоколы функционируют в сетях связи, основанных на стеке протоколов *TCP/IP*, что затрудняет их использование в ГСС, использующих отличный от *TCP/IP* стек протоколов передачи данных.

Алгоритмы сопряжения ГСС, описанные в настоящей работе, обосновывают необходимость разработки и внедрения дополнительного межсетевого протокола, обеспечивающего передачу адресов взаимодействующих сетей и узлов, и предназначенного для предоставления возможности внешним шлюзам осуществлять межсетевую коммутацию. Алгоритм сопряжение ГСС с использованием двух внешних шлюзов и транспортной сети обладает рядом преимуществ по сравнению с использованием централизованного внешнего шлюза. Одно из них заключается в том, что в каждом внешнем шлюзе необходимо реализовать только две базовые сетевые технологии – БСТ ГСС и БСТ транспортной сети, что упрощает его реализацию. Так же повышается масштабируемость системы в целом, при этом подключение или отключение внешних шлюзов к транспортной сети не затрагивает функционирование уже подключенных ГСС. В отличии от варианта с централизованным внешним шлюзом, нет необходимости выдавать единственному разработчику централизованного внешнего шлюза информацию обо всех «закрытых» БСТ, построение системы децентрализовано, что позволяет гибко обеспечивать требования безопасности информации.

Одновременно при построении вышеописанной архитектуры взаимодействия ГСС существуют и «тонкие» места, требующие дополнительного внимания и проработки. К таким проблемным вопросам относится, например, определение максимального объема данных (*MTU*), передаваемых по взаимодействующим ГСС и транспортной сети без дальнейшей фрагментации (одним пакетом). Для определения *MTU* при сопряжении ГСС потребуется определение минимального *MTU*, используемого в сети-отправителя, транспортной сети и сети-получателя, и назначить данный размер для MTU взаимодействующих систем. Также к проблемным вопросам можно отнести реализацию динамической маршрутизации во внешних шлюзах на уровне вновь разработанного межсетевого телекоммуникационного протокола.

Сопряжение множества гетерогенных сетей связи представляется нетривиальной задачей и предполагается, что данная работа послужит началом в разработке математического аппарата и методов объедения различных ГСС, а также поможет в разработке системно-технических решений по организации информационного обмена объектов информатизации, расположенных в различных ГСС.

Литература

1. Журнал «Воздушно-космическая оборона». Проблемы создания АСУ Вооруженных Сил. [Электронный ресурс] URL.:http://www.vko.ru/koncepcii/problemy-sozdaniya-asu-vooruzhennyh-sil (Дата обращения: 29.04.2021).

2. Николашин Ю.Л., Кулешов И.А. Предложения по методам сопряжения гетерогенных сетей связи специального назначения и их оценка // Техника средств связи. 2019. № 2 (146). С. 4-7.

3. Сетевые решения. Подходы к интеграции неоднородных сетей. Часть 1. [Электронный ресурс] URL.:https://nestor.minsk.by/sr/2000/06/00606.html (Дата обращения: 30.04.2021).

4. Макаренко С.И. Описательная модель сети связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 113-164. [Электронный ресурс] URL.:http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf (Дата обращения: 05.05.2021).

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

6. Олифер В.Г, Олифер Н.А., Компьютерные сети. Принципы, технологии, протоколы – СПб.: изд-во Питер, 2020. – 1008 с.

7. Щербо В.И. Протоколы маршрутизации Internet [Электронный ресурс] URL.:https://www.osp.ru/os/1999/11-12/177881 (Дата обращения: 06.05.2021).

References

1. Zhurnal "Vozdushno-kosmicheskaya oborona". Problemy sozdaniya ASU Vooruzhennyh Sil. URL.:http://www.vko.ru/koncepcii/problemy-sozdaniya-asu-vooruzhennyh-sil (accessed 29.04.2021) (in Russian).

2. Nikolashin Yu.L., Kuleshov I.A. Predlozheniya po metodam sopryazheniya geterogennyh setej svyazi special'nogo naznacheniya i ih ocenka. Means of communication equipment. 2019. № 2 (146). Pp. 4-7 (in Russian).

3. Setevye resheniya. Podhody k integracii neodnorodnyh setej. CHast' 1. URL.:https://nestor.minsk.by/sr/2000/06/00606.html (accessed 30.04.2021) (in Russian).

4. Makarenko S.I. Opisatel'naya model' seti svyazi special'nogo naznacheniya. Sistemy upravleniya, svyazi i bezopasnosti. 2017. № 2. Pp. 113-164. URL.:http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf (accessed 05.05.2021) (in Russian).

5. Infokommunikacionnye seti: enciklopediya. Kniga 4: Geterogennye seti svyazi: principy postroniya, metody sinteza, effektivnost', cena, kachestvo. P.A. Budko, I.A. Kuleshov, V.I. Kurnosov, V.I. Miroshnikov; pod red. professor V.I. Miroshnikova. Moscow. Nauka, 2020, 683 p. (in Russian).

6. Olifer V.G, Olifer N.A., Komp'yuternye seti. Principy, tekhnologii, protokoly. SPb.: Piter Publ., 2020. 1008 p. (in Russian).

7. Shcherbo V.I. Protokoly marshrutizacii Internet. URL.:https://www.osp.ru/os/1999/11-12/177881 (accessed 06.05.2021) (in Russian).

Статья поступила 10 мая 2021 г.

Информация об авторах

Кулешов Игорь Александрович – Доктор технических наук, доцент, заместитель генерального директора по научной работе ПАО «Интелтех». Тел.:+7 (812) 295-50-69. E-mail: intelteh@inteltech.ru.

Мержеевский Александр Александрович – Начальник отдела ПАО «Интелтех». Тел.:+7(812)295-50-69. E-mail: intelteh@inteltech.ru. Адрес: Санкт-Петербург, ул. Кантемировская, д. 8.

Algorithm for interfacing heterogeneous data transmission networks

I.A. Kuleshov, A.A. Merzheevskiy

Annotation: *The aim of the work is to determine a rational algorithm for interfacing heterogeneous data transmission networks that use different stacks of network protocols, taking into account the existing problems of their interaction. The paper presents an algorithm for interfacing two or more heterogeneous networks using external gateways. The advantages and disadvantages of interfacing networks using a centralized external gateway and a distributed external gateway are noted. The result of the work is a generalized algorithm for interfacing heterogeneous data transmission networks using the inter-network communication protocol and distributed external gateways. The practical significance of the work is aimed at determining the ways of applying existing and developing new methods for combining heterogeneous special-purpose data transmission networks.*

Keywords: *heterogeneous data transmission network, interface algorithm, external gateway, internetwork protocol.*

Information about the authors

Igor Aleksandrovich Kuleshov – Doctor of Technical Sciences, Associate Professor, Deputy General Director of PJSC "Inteltech" for scientific work. Tel.:+7 (812) 295-50-69. E-mail: intelteh@inteltech.ru.

Alexander Alexandrovich Merzheevsky – Head of the Department of PJSC "Inteltech". Tel.:+7 (812) 295-50-69, e-mail: intelteh@inteltech.ru. Address: St. Petersburg., Kantemirovskaya str., 8.

Для цитирования: Кулешов И.А., Мержеевский А.А. Алгоритм сопряжения гетерогенных сетей передачи данных // Техника средств связи. 2021. № 2 (154). С. 18-24.

For citation: Kuleshov I.A., Merzheevskiy A.A. Algorithm for interfacing heterogeneous data transmission networks. Means of Communication Equipment. 2021. No. 2 (154). Pp. 18-24 (in Russian).

УДК 621.396/395.74

Аппаратно-программные комплексы обеспечения устойчивости автоматизированной системы связи ВМФ

Талагаев В.И.

Аннотация: *Предложен методологический подход к обеспечению устойчивости системы связи Военно-Морского Флота, основанный на адаптации её структуры и параметров к деструктивным воздействиям, средств радиоэлектронного подавления радиоканалов, отказов технических средств ионизирующих излучений и электромагнитных импульсов на среду распространения сигналов и радиоэлектронное оборудование. Приведена архитектура встраиваемых в систему управления связью программно-технических комплексов адаптивного управления системой, радиосредствами береговых объектов связи, комплексами связи подводных лодок и надводных кораблей.*

Ключевые слова*: автоматизированная система связи, деструктивные и дестабилизирующие воздействия, адаптивное управление системой связи, аппаратно-программные средства адаптации к деструктивным воздействиям.*

Введение

Одной из сложных научно-технических проблем, возникающих в процессе исследований, создания и функционирования автоматизированной системы связи (АСС) Военно-Морского Флота (ВМФ) в различных оперативно-тактических ситуациях продолжает оставаться обеспечение ее устойчивости к разнородным внешним и внутренним деструктивным и дестабилизирующим факторам.

Устойчивость АСС ВМФ, как способность противостоять нарушению информационного обмена в системе, вследствие различных видов поражения объектов связи, радиоэлектронного подавления (РЭП) радиоканалов (РК), выхода из строя ненадежных аппаратно-программных средств, влияния ионизирующих излучений (ИИ) и электромагнитных импульсов (ЭМИ) на среду распространения сигналов и электронное оборудование может быть обеспечена путем адаптации АСС, т. е. подстройки ее структуры и параметров к указанным воздействиям средствами управления [1].

Отличительной особенностью современных методов адаптивного управления сложными динамическими системами является автоматизация этих процессов на основе широкого применения ЭВМ, требующая специального программного, информационного и технического обеспечения. Речь, таким образом, идет о представлении исследователям, проектировщикам и должностным лицам органов оперативного управления АСС набора программных и технических средств, позволяющих в автоматическом или ручном режимах подстраивать действующую систему к прогнозируемым или фактическим деструктивным воздействиям, т. е. выбирать оптимальную с точки зрения устойчивости структуру АСС с учетом разнородных деструктивных воздействий. Цель адаптации – поддержание требуемого для управления силами и средствами ВМФ качества функционирования АСС путем компенсации и восстановления потерь качества, вызванного деструктивными факторами.

1. Адаптивное управление структурой автоматизированной системы связи в условиях деструктивных воздействий

Адаптация, как подстройка структуры и параметров АСС к прогнозируемым или фактическим деструктивным воздействиям, достигается путем изменения ее внутреннего состояния, адекватного воздействиям. Адаптация системы к воздействиям может быть обеспечена при наличии в АСС организационно-технического ресурса (основного и резервного), структурной и функциональной избыточности относительно минимального их состава, необходимого для функционирования системы с требуемым качеством в *i*-ый период

$K_{фi} = K_{трi}$ в отсутствие воздействий $\Delta K_{Bi} = 0$ ($\Delta K_{изб} = K_{фмах}$, $K_{фi}$). Практически изменение внутреннего состояния АСС сводится к перераспределению связных ресурсов и потоков сообщений, к которым относятся основные и резервные средства связи и режимы их работы.

Способность АСС обеспечивать на всех этапах жизненного цикла требуемое качество функционирования в условиях комплексного воздействия деструктивных факторов определяется как устойчивость системы к воздействиям (живучесть), средств разведзащищенности, средств РЭП (помехозащищенность), отказов технических средств (надежность) и ошибок эксплуатации и управления (верность, правильность). Свойство устойчивости проявляется только в условиях воздействий (по отношению к воздействиям) и обеспечивается разными видами избыточности, вводимыми в АСС на этапах ее проектирования и разработки. Избыточность в виде пассивных мер (механическая защита объектов, резервирование технических средств, использование высоконадежной помехозащищенной аппаратуры и др.) и активных мер (адаптивные методы управления, изменение структуры и организации ее использования, маневрирование частотным ресурсом и режимами работы оборудования и др.) вводится в АСС (в ее структуру и алгоритмы функционирования и управления). Величина избыточности $\Delta K_{М}$ выбирается с учетом требований к качеству функционирования при максимальных прогнозируемых воздействиях $K_{фмах} = K_{ф} + \Delta K_{М}$ и реализуется на этапах функционирования в виде совокупности организационно-технических мероприятий, адекватных фактическим деструктивным воздействиям в i-ый период работы $\Delta K_{М} = \Delta K_{Bi}$ [2].

Рекомендации проектировщику, должностным органам оперативного управления АСС и исполнительным элементам в системах автоматизированного управления по изменению структуры АСС и ее параметров могут быть выработаны в результате комплексного решения на ЭВМ двух основных расчетно-логических задач:

1) Расчетной задачи анализа по определению и сравнению с требуемым для эффективного управления силами обобщенного показателя устойчивости АСС к прогнозируемым и заданным моделью (при проектировании) и фактическим (текущим при функционировании АСС в реальных условиях) внешним и внутренним деструктивным и дестабилизирующим воздействиям на циклах управления;

2) Расчетно-логической задачи синтеза по выбору перспективного варианта структуры АСС и ее параметров, обеспечивающих требуемую для управления силами и средствами устойчивость АСС с учетом фактического и прогнозируемого, задаваемого моделью состояния системы при внешних и внутренних деструктивных воздействиях.

Решение первой задачи заключается в комплексной оценке устойчивости АСС в данном состоянии структуры системы с учетом матриц поражения различными видами воздействий объектов связи, РК преднамеренными помехами, влияния ИИ и ЭМИ на радиоканалы и аппаратуру, выхода из строя технических средств и сравнения ее значения с предельно допустимым (требуемым для эффективного управления силами). Оценка устойчивости является комплексной и производится на основе расчета живучести объектов связи, помехозащищенности РК, влияния ИИ и ЭМИ на РК, надежности технических средств системы на основе оценки снижения качества функционирования АСС в результате этих воздействий. При снижении устойчивости ниже требуемой, исследователем или оператором связи должно приниматься решение об изменении структуры и переводе АСС в новое перспективное состояние.

Определение перспективной, наилучшей при заданном воздействии структуры АСС, обеспечивающей требуемую устойчивость – вторая расчетно-логическая задача адаптивного управления АСС. В общем виде задача относится к классу экстремально поисковых [3] и может быть решена методами математического программирования. Поскольку АСС является сложной динамической системой, полная формализация процессов, происходящих в ней, и их строгий анализ вызывает значительные трудности, то для решения расчетной и расчетно-

логических задач на этапе исследований и оперативного управления АСС целесообразно использовать расчетно-логическую и экспертную системы [4].

Экспертная система в данном случае – это совокупность программно-реализованных моделей, обеспечивающих проведение анализа устойчивости и выдачу рекомендаций по выбору оптимальной структуры АСС и ее параметров в условиях прогнозируемого и фактического деструктивных воздействий. Анализ состояния системы и рекомендации по изменению её структуры и параметров основаны на редуцировании (обобщении) аналитических расчетов, опыте эксплуатации и знаний экспертов по связи, способных сделать оценку устойчивости и выдвинуть вполне надежные предложения по оптимизации структуры и ее параметров неполной информации об АСС, деструктивном прогнозируемом и фактическом воздействии на нее при отсутствии формальных средств их описания. Несмотря на субъективный характер, знания экспертов имеют особую ценность, поскольку содержат все, что, хотя бы частично осознано, но еще не сформулировано в строгом виде.

Для решения второй расчетно-логической задачи необходима совокупность аппаратно-программных средств, позволяющих исследователю или оператору связи решать задачи анализа устойчивости АСС и ее свойств (живучести, развед- и помехозащищенности, устойчивости к ИИ и ЭМИ, надежности оборудования связи) и оптимизации структуры по их постановке и описанию в терминах радиосвязи, пользуясь услугами специалистов связи, алгоритмистов и программистов. Для такой системы характерно наличие модели АСС, моделей внешних воздействий, условий функционирования и специальной программы-планировщика вычислений. Использование расчетно-логической системы делает доступной для исследователя, проектанта и оператора связи реализацию прикладных математических методов расчета на ЭВМ в целях анализа устойчивости и выбора по его результатам наилучшей структуры АСС в процессе ее разработки и функционирования, т. е. изменения интенсивности потоков сообщений, характера внешних воздействий и оперативно-тактических ситуаций.

Для решения этой задачи необходимо располагать прогнозом, или изменяющимися данными о текущем состоянии АСС, т. е. об огневом поражении объектов связи, подавлении РК АСС преднамеренными помехами и техническом состоянии радиосредств, получаемые от программно-технических средств мониторинга АСС. Для решения задачи, кроме того, необходимо располагать постоянной информацией, т. е. моделями потенциально возможного огневого, помехового, ИИ и ЭМИ воздействий противника на АСС и др. Требования к программно-аппаратным средствам решения задач адаптации АСС, необходимых при проведении исследований и при оперативном управлении системой различаются. При исследованиях важна полнота учета возможных операционно-тактических ситуаций (множества вариантов) и адекватных расчетно-логических моделей реальным условиям функционирования АСС, а при оперативном управлении действующей АСС – быстрота принятия решений по изменению структуры системы. Поэтому при проведении исследований и проектировании АСС данные о внешних воздействиях могут быть получены с помощью их имитаторов, а при оперативном управлении от средств мониторинга состояния – датчиков состояния объектов и каналов связи. Эти сведения могут храниться в единой базе данных, служащей основой информационного обеспечения для решения расчетной и расчетно-логической задач.

2. Структура аппаратно-программных комплексов адаптации АСС к воздействиям

Характер внешних воздействий определяется оперативно-тактической обстановкой, поэтому при решении обеих задач адаптации АСС к условиям функционирования необходимо так же учитывать состав, пространственное расположение и действия сил и средств противника. При проведении исследований и проектировании АСС, оперативно-тактическая ситуация может быть задана в виде набора сценариев действий сил и средств, и

хранится так же в единой базе данных, а в действующую АСС может вводиться извне в ее расчетно-логическую систему от системы освещения оперативно-тактической обстановки.

Необходимыми исходными данными для решения указанных задач являются информация о состоянии компонентов АСС и характера деструктивных и дестабилизирующих воздействий, которые должны поступать в систему управления от комплекса аппаратно-программных средств мониторинга и отображения состояния системы и ее компонентов. Аппаратно-программные средства могут встраиваться в автоматизированную систему управления или использоваться автономно при ручном управлении, как средства интеллектуальной поддержки должностных лиц органов управления АСС.

Встроенные в систему управления АСС аппаратно-программные средства, решающие указанные задачи адаптации, являются средствами автоматизации управления АСС и служат повышению устойчивости к внутренним и внешним воздействиям, обеспечивая тем самым требуемое качество информационного обмена в любых оперативно-тактических условиях. На первом этапе автоматизации функций адаптации АСС к разнородным деструктивным воздействиям программно-аппаратные комплексы могут использоваться как средства интеллектуальной поддержки должностных лиц органов планирования связи на операции и оперативного управления действующей АСС.

Обобщенная структура и состав программно-технических средств обеспечения управления АСС, локальной сетью, бортовыми комплексами связи кораблей в условиях деструктивных воздействий приведены на рис.

Предложенный методологический подход к построению программных и аппаратных средств интеллектуальной поддержки должностных лиц органов управления АСС ВМФ в условиях внешних и внутренних деструктивных воздействий и отдельные программные и технические средства реализации процессов адаптивного управления АСС ВМФ приведены в работах [5-11].

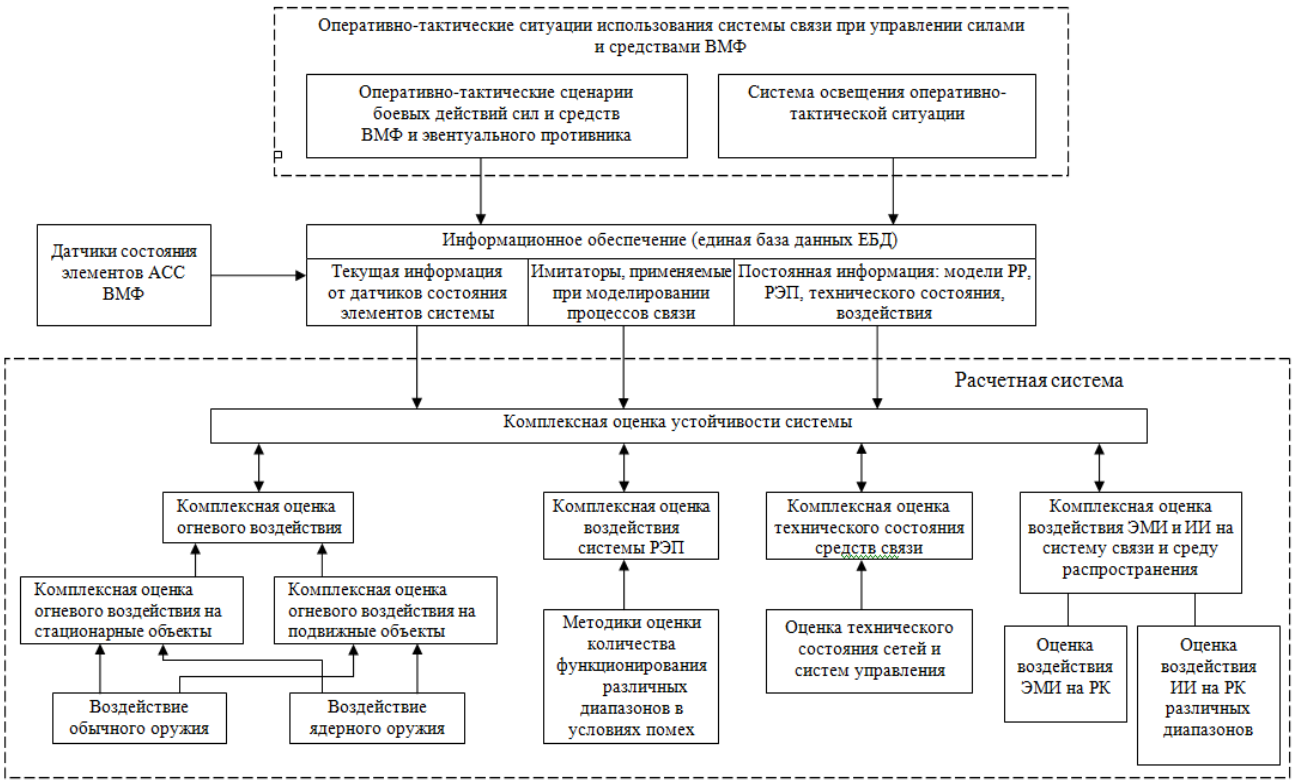


Рис. Архитектура аппаратно-программных средств адаптивного управления АСС, в условиях деструктивных воздействий

Выводы

Аппаратно-программные комплексы обеспечения устойчивости АСС относятся к интеллектуальным средствам автоматизации управления при адаптации ее структуры и параметров к разнородным внешним и внутренним деструктивным и дестабилизирующим факторам.

Комплексы представляет собой совокупность общих информационных и программных (расчетно-логических и экспертных) моделей, позволяющих производить оценку устойчивости АСС и вырабатывать рекомендации по выбору ее наилучшей структуры и её параметров как при проведении исследований и проектировании, так и при планировании связи на операции флота и управлении АСС ВМФ в реальных условиях.

Предложенная методология и структура программно-технических комплексов обеспечения устойчивости АСС ВМФ могут применяться также при автоматизации и интеллектуализации управления полевыми сетями связи и их компонентами с учетом оперативно-тактических особенностей их организации и использования.

Литература

1. Талагаев В.И. Управление системой связи и обмена данными ВМФ в условиях радиоэлектронного подавления // Техника средств связи. 2018. № 4 (144). С. 130-134.

2. Талагаев В.И. Методологический подход к анализу и обеспечению устойчивости систем морской радиосвязи // Техника средств связи. 2018. № 3 (143). С. 86-91.

3. Евтушенко Ю.Т. Методы решения экстремальных задач и их применении в системах оптимизации. – М.: Наука, 1982. 432 с.

4. Мирошников В.И., Кулешов И.А., Талагаев В.И. Экспертная система оценки помехозащищённости декаметровых радиоканалов ВМФ // Техника средств связи. 2020. № 2 (150). С. 26-33.

5. Николашин Ю.Л., Гавриленко С.А., Талагаев В.И. Модель анализа помехозащищенности направления связи с морскими объектами. Часть 1 // Морская радиоэлектроника. 2018. № 2 (64). С. 34-37.

6. Николашин Ю.Л., Гавриленко С.А., Талагаев В.И. Модель анализа помехозащищенности направления связи с морскими объектами. Часть 2 // Морская радиоэлектроника. 2018. № 3 (65). С. 44-47.

7. Талагаев В.И., Лебедев Д.В. Выбор безопасных рабочих частот для декаметровых каналов связи в условиях радиоразведки и радиоэлектронного подавления. Тематический научно-технический сборник ФГУП «24 ЦНИИ МО», Санкт-Петербург, 2011.

8. Гавриленко С.А., Талагаев В.И., Лебедев Д.В. Программа оценки помехозащищенности направлений связи с морскими объектами v.1.0. Свидетельство о государственной регистрации программы для ЭВМ № 2013614725 от 20.05.2013, ФГБУ ФИПС, Москва, 2013.

9. Талагаев В.И., Лебедев Д.В. Программа для анализа потенциальных возможностей радиоразведки v.1.0. Свидетельство о государственной регистрации программы для ЭВМ № 2014611242 от 28.01.2014, ФГБУ ФИПС, Москва, 2014.

10. Талагаев В.И., Лебедев Д.В. Модель выбора трасс каналов в региональной сети связи. Свидетельство о государственной регистрации программы для ЭВМ № 2018619211 от 02.08.2018, ФГБУ ФИПС, Москва, 2018.

11. Талагаев В.И., Кезлинг А.Г. Способ контроля состояния дискретного радиоканала. Патент РФ на изобретение № 2003235, ФГБУ ФИПС, Москва, 1993.

References

1. Talagaev V.I. Management of the Navy communication and data exchange system in the conditions of electronic suppression. Means of communication equipment. 2018. № 4 (144). P. 130-134 (in Russian).

2. Talagaev V.I. Methodological approach to analysis and ensuring the stability of marine radio communication systems. Means of communication equipment. 2018. № 3 (143). P. 86-91 (in Russian).

3. Yevtushenko Yu.T. Methods of solving extreme problems and their application in optimization systems. Moscow. Science, 1982. 432 p. (in Russian).

4. Miroshnikov V.I., Kuleshov I.A., Talagaev V.I. Expert system for assessing the noise immunity of decameter radio channels of the Navy. Means of communication equipment. 2020. № 2 (150). P. 26-33 (in Russian).

5. Nikolashin Yu.L., Gavrilenko S.A., Talagaev V.I. Model of analysis of noise immunity of communication direction with marine objects. Part 1. Marine radio electronics. 2018. № 2 (64). P. 34-37 (in Russian).

6. Nikolashin Yu.L., Gavrilenko S.A., Talagaev V.I. Model of analysis of noise immunity of communication direction with marine objects. Part 2.Marine radio electronics. 2018. № 3 (65). P. 44-47 (in Russian).

7. Talagaev V.I., Lebedev D.V. Selection of safe operating frequencies for decameter communication channels in conditions of radio reconnaissance and electronic suppression. Thematic scientific and technical collection of FSUE "24 Central Research Institute of Economics," St. Petersburg, 2011 (in Russian).

8. Gavrilenko S.A., Talagaev V.I., Lebedev D.V. Program for assessing the noise immunity of communication directions with marine objects v.1.0. Certificate of state registration of the program for computers No. 2013614725 dated 20.05.2013, FSBI FIPS, Moscow, 2013 (in Russian).

9. Talagaev V.I., Lebedev D.V. Program for analysis of potential capabilities of radio exploration v.1.0. Computer Program State Registration Certificate No. 2014611242 dated 28.01.2014, FSBI FIPS, Moscow, 2014 (in Russian).

10. Talagaev V.I., Lebedev D.V. Model of selection of channel routes in the regional communication network. Certificate of state registration of the program for computers No. 2018619211 of 02.08.2018, FSBI FIPS, Moscow, 2018 (in Russian).

11. Talagaev V.I., Kezling A.G. Method of monitoring the state of a discrete radio channel. Patent of the Russian Federation for invention No. 2003235, FSBI FIPS, Moscow, 1993 (in Russian).

Статья поступила 07 мая 2021 г.

Информация об авторе

Талагаев Владимир Иванович – Кандидат технических наук, старший научный сотрудник, профессор Академии военных наук. Ведущий научный сотрудник ПАО «Интелтех». Тел.: +7(812) 448-96-50. E-mail: TalagaevVI@inteltech.ru. Адрес: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

Stability Hardware and Software Packages Navy Automated Communication System

V.I. Talagaev

Annotation: *A methodological approach to ensuring the stability of the Navy communication system is proposed, based on the adaptation of its structure and parameters to destructive effects, means of electronic suppression of radio channels, failures of technical means of ionizing radiation and electromagnetic pulses to the medium of signal propagation and radioelectronic equipment. The architecture of software and technical systems of adaptive control of the system, radio means of coastal communication facilities, communication systems of submarines and surface ships embedded in the communication control system is given.*

Keywords: *automated communication system, destructive and destabilizing effects, adaptive control of communication system, hardware and software means of adaptation to destructive effects.*

Information about Autor

Vladimir Ivanovich Talagaev – Candidate of Technical Sciences, Senior Researcher, Professor of the Academy of Military Sciences. Leading researcher at PJSC «Inteltech». Tel.: +7 (812) 448-96-50. E-mail: TalagaevVI@inteltech.ru. Address: 197342, Russia, St. Petersburg, 8 Kantemirovskaya St.

Для цитирования: Талагаев В.И. Аппаратно-программные комплексы обеспечения устойчивости автоматизированной системы связи ВМФ // Техника средств связи. 2021. № 2 (154). С. 25-30.

For citation: Talagaev V.I. Stability Hardware and Software Packages Navy Automated Communication System. Means of Communication Equipment. 2021. No. 2 (154). Pp. 25-30 (in Russian).

МОДЕЛИРОВАНИЕ СЛОЖНЫХ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ

УДК 621.61; 623.61

Модель построения телекоммуникационной сети специального назначения

Мержеевский А.А., Спивак А.И., Львов А.Е.

Аннотация. *В работе приведена актуальность моделирования телекоммуникационной сети специального назначения и представлены ее назначение и основные задачи. Описаны модели построения телекоммуникационной системы, а также сформулированы требования к телекоммуникационной сети специального назначения, на основе которых разработаны основные принципы ее построения. На основе анализа требований и принципов построения телекоммуникационной сети специального назначения в работе рассмотрены подходы к формированию модели, основные из которых включают декомпозицию объекта исследования (телекоммуникационной сети специального назначения), формирование трактов прохождения сообщений, определение исходящего трафика сообщений. Моделируемые уровни телекоммуникационной сети специального назначения представлены в соответствии с семиуровневой моделью OSI. На основе полученных данных сделан вывод, что в математической модели средства обеспечения безопасности будут оказывать влияние только на временные характеристики (время, затрачиваемое на проверку легитимности пакета, шифрование/дешифрование и т. д.). Таким образом, совокупность алгоритмов передачи транспортного уровня и рассмотренных математических моделей канального и сетевого уровней образует модель телекоммуникационной системы. Объединение модели телекоммуникационной системы с моделью трафика пользователя, позволит оценить соответствие предлагаемых технических решений потребностям пользователей сети, с учетом их дальнейшего роста и развития. Далее рассматриваются задачи, решение которых должно быть отражено в модели. Таким образом телекоммуникационная система специального назначения, построенная и развернутая на основании предложенной модели, учитывающей влияние различных факторов, повысит эффективность управления войсками, поскольку сэкономленное на обработке и передаче время уменьшит общее время реакции на изменение окружающей обстановки. Для подготовки статьи были использованы подходы, рассмотренные отечественными авторами: Гнеденко Б.В., Коваленко И.Н., Вентцель Е.С.*

Ключевые слова*: телекоммуникационная сеть специального назначения, модель телекоммуникационной системы, модель трафика пользователей, требования к телекоммуникационной системе, принципы построения.*

Введение

Техническое и информационное обеспечение Вооруженных Сил Российской Федерации (ВС РФ) является составной частью общей системы военного строительства государства и поэтому должно базироваться на использовании современных методов передачи и защиты информации с предоставлением широкого спектра услуг связи.

Особенно остро данная проблема проявляется на фоне непрекращающейся экспансии военного контингента США и стран НАТО в сторону российских границ. Одним из приоритетных направлений современного военного строительства государства является увеличение боевой мощи и качественное повышение эффективности органов и пунктов управления ВС РФ, обеспечивающих решение задач национальной безопасности и территориальной целостности страны.

В действительности оперативное и качественное выполнение этих задач предопределяет необходимость оснащения ВС РФ не только современными видами вооружений, но и распределенными автоматизированными системами управления войсками, краеугольной составляющей которых является телекоммуникационная инфраструктура.

1. Описание телекоммуникационной сети специального назначения

Основной составляющей любой телекоммуникационной инфраструктуры является телекоммуникационная сеть (ТКС).

Телекоммуникационную сеть, создаваемую в интересах спецпотребителей [1, 2], как правило называют ТКС специального назначения (СН). Она предназначена прежде всего для:

обеспечения управления войсками в ВС РФ;

предоставления должностным лицам и органам военного управления современных информационных и телекоммуникационных услуг;

создания единого инфокоммуникационного пространства интеллектуальных сетей интегрального обслуживания;

формирования открытых и защищенных мультимедийных сетей, базирующихся на объектовых сетях, сетях доступа и транспортной сети;

обеспечения требуемого качества связи за счет применения цифровых способов приоритетной передачи, хранения, распределения и обработки информации, а также оперативного управления данными процессами;

устойчивого функционирования в условиях воздействия на ее элементы различных видов оружия противника, опасных факторов техногенного и природного характера и всех видов помех.

Уровень реализации и развития потенциальных боевых возможностей системы управления войсками становится в более значительной степени зависимым от надежности и эффективности функционирования именно телекоммуникационной сети и ее способности обеспечивать своевременный, достоверный, устойчивый и безопасный информационный обмен между территориально разнесенными объектами: командными пунктами, штабами и т. д.

Каналы связи, предоставляемые операторами связи, активно используются в составе телекоммуникационной инфраструктуры ВС РФ, что создает реальные угрозы перехвата и модификации информации, отслеживания и анализа трафика, разрушения телекоммуникационной инфраструктуры системы управления ВС РФ.

Принятая ранее телекоммуникационная инфраструктура, построенная на выделенных каналах связи, в настоящее время существенно отстает от потребностей системы управления войсками, что позволяет говорить о постоянном превосходстве противника, достигаемом и удерживаемом за счет качества оперативного управления – полноты, глубины, оперативности знания, единого понимания и оценки динамично развивающейся обстановки командованием всех уровней, а также быстроты реагирования на изменяющуюся ситуацию принятием своевременных обоснованных решений и ускоренного доведения их до соответствующих объектов боевого управления.

Требования к ТКС СН можно сформулировать следующим образом [2]:

сеть должна разрабатываться с учетом анализа тенденций, текущего и ожидаемого уровней развития информационно-телекоммуникационных систем вооруженных сил наиболее технологически продвинутых государств и необходимости обеспечения опережающего ее развития по сравнению с аналогичными зарубежными системами;

сеть должна учитывать текущее состояние и тенденции развития телекоммуникационных технологий в мире и России;

сеть должна отвечать требованиям оперативности передачи информации при заданном уровне помех;

сеть должна удовлетворять специальным требованиям, предъявляемым к системам связи специального назначения, а именно устойчивого функционирования телекоммуникационной сети в мирное время, мобилизационный период и военное время.

При построении современной телекоммуникационной сети специального назначения необходимо придерживаться следующих принципов:

сеть должна базироваться на передовой технологии передачи информации (пакетной);

сеть должна отвечать современным требованиям системы управления войсками по вероятностно-временным характеристикам доставки сообщений;

сеть должна передавать все виды информации (голос, видео, данные);

телекоммуникационный трафик должен обрабатываться в соответствии с заданным качеством обслуживания.

Проектирование телекоммуникационной сети специального назначения является достаточно сложным и многогранным процессом ввиду необходимости учета множества факторов и критериев, оказывающих существенное влияние на ее функционирование.

Специальные требования, предъявляемые к системам специального назначения, обуславливают целый ряд дополнительных критериев, вытекающих из необходимости обеспечивать своевременный и надежный обмен информацией между объектами ТКС СН в мирное время, мобилизационный период и военное время в условиях ведения противником информационной, разведывательно-диверсионной и радиоэлектронной борьбы [3].

С помощью модели телекоммуникационной сети можно предположить реакцию реальной сети на ряд возникающих ситуаций. Зная количество межобъектового трафика и прогнозируя его будущую тенденцию, можно построить современную ТКС специального назначения. Модель должна отражать решение задач своевременного, достоверного и безопасного обмена данными реального времени.

В общем виде процесс моделирования телекоммуникационной сети приведен на рис. 1.

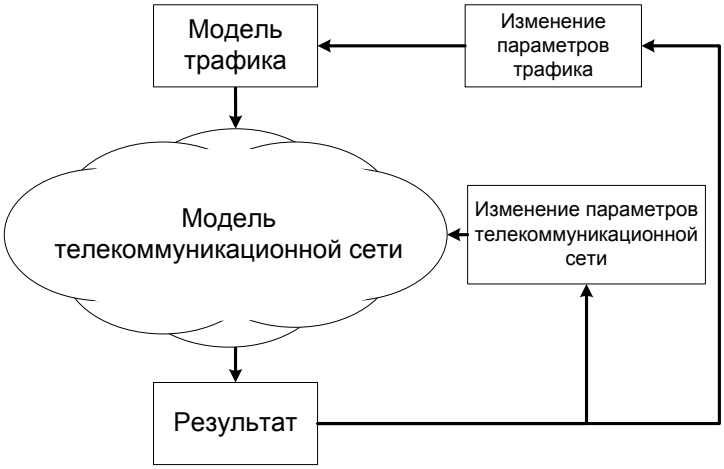


Рис. 1. Процесс моделирования телекоммуникационной сети

Для упрощения проектирования и анализа логической архитектуры ТКС СН осуществляется декомпозиция структуры сети на сквозные тракты передачи информации (СТПИ), представляющие собой цепочки элементов телекоммуникационной сети (средства обеспечения безопасности, коммутаторы, маршрутизаторы и т. п.), образующие пути передачи информации между удаленными объектами. Для анализа характеристик передачи информации в телекоммуникационной сети из множества СТПИ выбираются наихудшие по характеристикам тракты, включающие наибольшее число переприемных элементов, наихудшие по качеству каналы связи и т. д. Общий вид ТКС СН и ее декомпозиция на СТПИ представлены на рис. 2 и 3 соответственно.

Каждый участок СТПИ (канал, средство обеспечения безопасности, маршрутизатор) характеризуется своими вероятностно-временными характеристиками, в совокупности с которыми алгоритмы передачи информации образуют модель телекоммуникационной сети [2, 3]. Моделируемые в данной статье уровни телекоммуникационной сети специального назначения, в соответствии с семиуровневой моделью *OSI*, представлены на рис. 4.

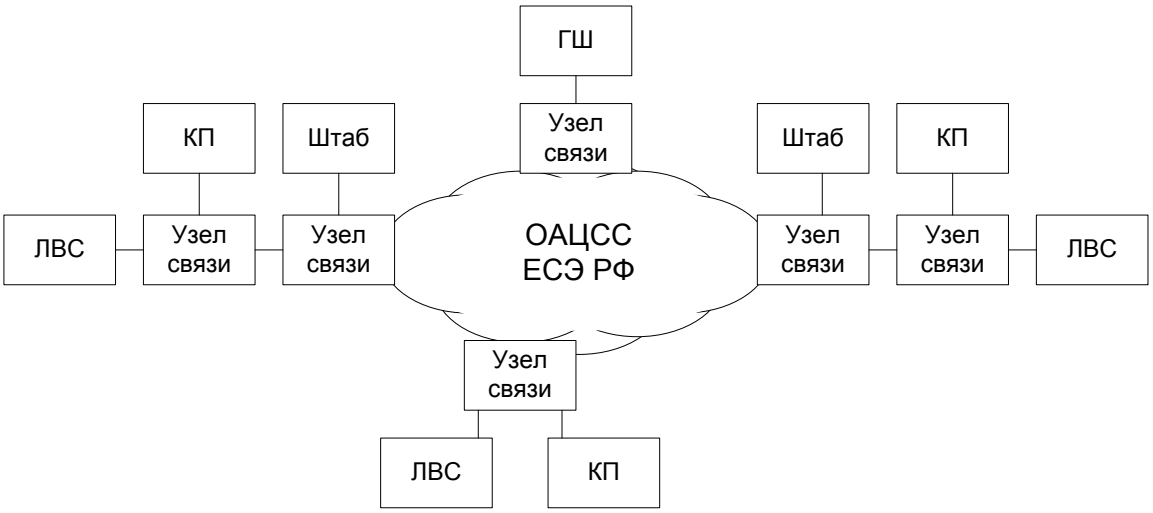


Рис. 2. Общий вид телекоммуникационной сети специального назначения

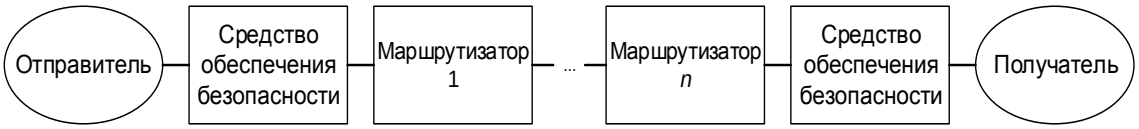


Рис. 3. Декомпозиция телекоммуникационной сети на СТПИ

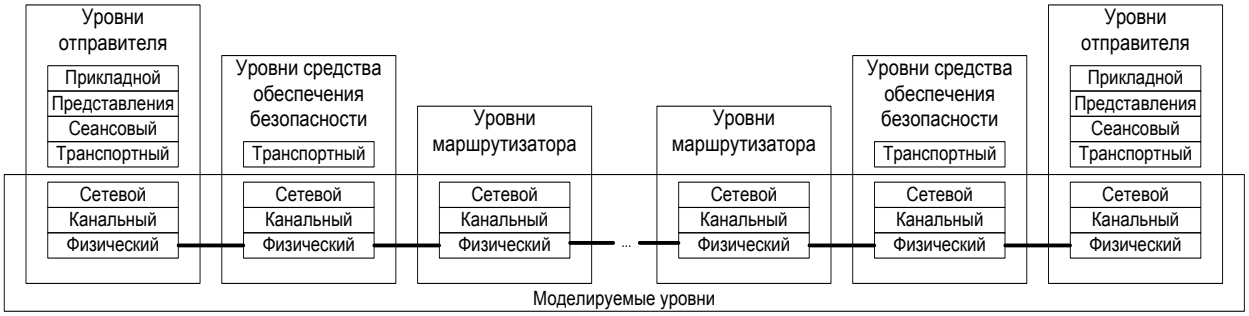


Рис. 4. Проецирование СТПИ на семиуровневую модель *OSI*

2. Модель телекоммуникационной сети специального назначения

Предположим, что на канальном уровне, в соответствии с семиуровневой моделью *OSI*, сеть осуществляет передачу данных по протоколу *Ethernet*, тогда вероятность доставки кадра (пакет, обрамленный служебной информацией канального уровня) зависит от вероятности искажения бит в полученном кадре [4]:

$$P_{KC_o} = \left(1 - P_{\text{бит.ош.}}\right)^N,$$

где $P_{\text{бит.ош.}}$ – вероятность битовой ошибки в канале связи, предполагаем априори известной; $N = m \cdot 8$ – размер кадра в битах (m – число байт в кадре).

Таким образом, вероятность доставки пакета через все каналы связи, встречающиеся в СТПИ, от отправителя до получателя вычисляется по следующей формуле:

$$P_{KC\text{общ}_o} = \prod_{i=1}^{k} P_{KC i_o},$$

где $i = \overline{1,k}$ – количество каналов связи, в СТПИ.

Средства обеспечения безопасности являются рубежом защиты от воздействия внешних нарушителей. Они обеспечивают конфиденциальность и целостность

циркулирующей между объектами телекоммуникационной сети информации и защиту телекоммуникационного оборудования объектов сети от внешних разрушающих воздействий. Предполагается, что производительность данных средств превышает поступающий поток пакетов. На базе данного предположения можем сделать вывод, что в математической модели средства обеспечения безопасности будут оказывать влияние только на временные характеристики (время, затрачиваемое на проверку легитимности пакета, шифрование/дешифрование и т. д.).

На сетевом уровне, в соответствии с семиуровневой моделью *OSI* решаются задачи маршрутизации телекоммуникационного трафика. Решение этих задач возложено на маршрутизаторы объектовых и магистральных сетей. В математической модели маршрутизатор можно представить в виде «черного ящика», в который входит множество пакетов от различных абонентов. Все множество пакетов обрабатывается в соответствии с заранее заложенными правилами. Схематично работа маршрутизатора представлена на рис. 5.

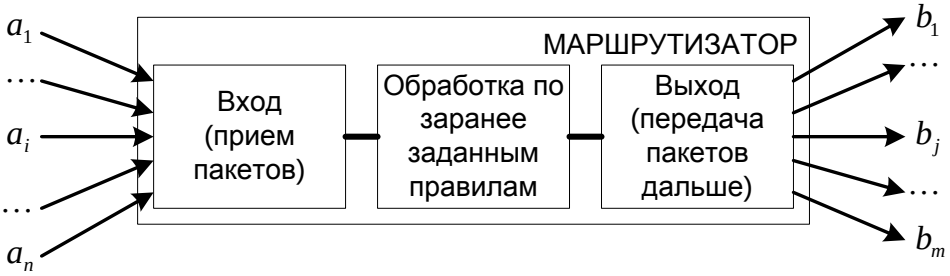


Рис. 5. Схематичное представление работы маршрутизатора

На рис. 5 представлены: $a = \sum_{i=1}^{n} a_i$ – количество входящих пакетов, $b = \sum_{j=1}^{m} b_j$ – количество выходящих пакетов, где $a \geq b$, это обусловлено тем, что входящие пакеты могут быть отброшены, если производительность маршрутизатора окажется ниже интенсивности поступающих на вход пакетов. Таким образом, вероятность потерь в маршрутизаторе не зависит от времени поступления пакета, она зависит от интенсивности поступающих пакетов, производительности и объема входного буфера маршрутизатора.

Вероятность потерь в маршрутизаторе можно описать следующим выражением [4]:

$$P_{m+r} = \frac{\frac{\rho^{m+r}}{m! m^r}}{\left(\sum_{k=0}^{m} \frac{\rho^k}{k!} + \frac{\rho^m}{m!} \sum_{s=1}^{r} \left(\frac{\rho}{m} \right)^s \right)},$$

где r – количество мест во входном буфере, m – количество одновременно обрабатываемых пакетов, k – количество пакетов находящихся в маршрутизаторе, $\rho = \frac{\lambda}{\mu}$ – увеличение нагрузки, λ – параметр входного потока (количество пакетов в единицу времени), μ – параметр обрабатываемого потока (величина обратная среднему времени обслуживания), s – количество освободившихся в буфере мест.

Обобщив ранее полученный результат можно сказать, что вероятность прохождения пакета через все $i = \overline{1,n}$ маршрутизаторов СТПИ будет равна [5]:

$$P_{\text{М}} = \prod_{i=1}^{n} \left(1 - P_{m+r}\right)_i .$$

Следовательно, вероятность прохождения пакета по СТПИ от отправителя до получателя будет вычисляться по следующей формуле:

$$P_{\text{ПП}} = P_{КСобщ_ц} \cdot P_{\text{М}} .$$

Пользовательские приложения прикладного уровня, могут использовать разные алгоритмы передачи информации на транспортном уровне: алгоритм с обратной связью (производится перезапрос поврежденных или недостающих пакетов) и алгоритм без обратной связи (для передачи речи, видео и т. п. в реальном времени). В зависимости от выбора алгоритма работы транспортного уровня, с учетом вероятности доставки пакетов на канальном и сетевом уровнях, можно получить вероятность передачи пользовательских сообщений.

Совокупность алгоритмов передачи транспортного уровня и рассмотренных математических моделей канального и сетевого уровней образует модель ТКС. Объединение модели ТКС с моделью трафика пользователя, позволит оценить соответствие предлагаемых технических решений потребностям пользователей сети, с учетом их дальнейшего роста и развития.

Вывод

Телекоммуникационная сеть специального назначения, построенная и развернутая на основании подробно проработанной модели телекоммуникационной сети, учитывающей влияние различных факторов, повысит эффективность управления войсками, поскольку сэкономленное на обработке и передаче время уменьшит общее время реакции на изменение окружающей обстановки.

Литература

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

2. Словарь войск связи ВС РФ./ Под ред. Карпова Е.А. – М. Воениздат, 2008. – 216 с.

3. Асеев А. А., Дудник Б. Я., Кулешов И. А. Проблемы организации военной связи. // Военная мысль. 2005. №2. С. 31- 40.

4. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. – М.: Изд-во ЛКИ, 2007. – 400 с.

5 Вентцель Е.С. Теория вероятностей. – М.: Физматлит, 1962. – 564 с.

References

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

2. Dictionary of the signal troops of the Armed Forces of the Russian Federation. / Ed. E.A. Karpov M. Voenizdat, 2008, 216 p. (in Russian).

3. Aseev A. A., Dudnik B. Ya., Kuleshov I. A. Problems of the organization of military communications. // Military thought. 2005. No. 2. Pp. 31-40. (in Russian).

4. Gnedenko B. V., Kovalenko I. N. Introduction to the theory of queuing. Moscow: LKI Publishing House, 2007. 400 p. (in Russian).

5 Wentzel E. S. Probability theory. M.: Fizmatlit, 1962, 564 p. (in Russian).

Статья поступила 22 мая 2021 г.

Информация об авторах

Мержеевский А.А. – Начальник отдела ПАО «Интелтех». E-mail: intelteh@inteltech.ru. Тел.:+7 (812) 313-12-51.

Спивак А.И. – Начальник отдела Центра защиты Государственной тайны НЦУО МО РФ. E-mail: intelteh@inteltech.ru. Тел.:+7(812) 313-12-51.

Львов А.Е. – начальник отдела Спецсвязи ФСО России. E-mail: intelteh@inteltech.ru. Тел.: +7 (812) 313-12-51.

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

Model of building a special-purpose telecommunications network

A.A. Merzheevsky, A.I. Spivak, A.E. L´vov

Annotation. *The paper presents the relevance of modeling a special-purpose telecommunications network and presents its purpose and main tasks. The models of building a telecommunications system are described, as well as the requirements for a special-purpose telecommunications network are formulated, on the basis of which the basic principles of its construction are developed. Based on the analysis of the requirements and principles of building a special-purpose telecommunications network, the paper considers approaches to the formation of a model, the main of which include the decomposition of the object of research (a special-purpose telecommunications network), the formation of message paths, the determination of outgoing message traffic. The simulated levels of a special-purpose telecommunications network are presented in accordance with the seven-level OSI model. Based on the data obtained, it is concluded that in the mathematical model, security tools will only affect the time characteristics (the time spent on verifying the legitimacy of the packet, encryption/decryption, etc.). Thus, the combination of transport layer transmission algorithms and the considered mathematical models of the channel and network levels forms a model of a telecommunications system. Combining the telecommunications system model with the user traffic model will allow us to assess the compliance of the proposed technical solutions with the needs of network users, taking into account their further growth and development. Next, the problems are considered, the solution of which should be reflected in the model. Thus, a special-purpose telecommunications system built and deployed on the basis of the proposed model, taking into account the influence of various factors, will increase the efficiency of troop management, since the time saved on processing and transmission will reduce the overall reaction time to changes in the environment. For the preparation of the article, the approaches considered by domestic authors were used: Gnedenko B. V., Kovalenko I. N., Wentzel E. S.*

Keywords: *special-purpose telecommunications network, telecommunications system model, user traffic model, requirements for a telecommunications system, principles of construction.*

Information about Autors

Merzheevsky A.A. – Head of Department of PJSC Inteltekh. E-mail: intelteh@inteltech.ru. Tel.: +7 (812) 313-12-51.

Spivak A.I. – Head of the Department of the Center for the Protection of State Secrets of the NCUO of the Ministry of Defense of the Russian Federation. E-mail: intelteh@inteltech.ru. Tel.: +7 (812) 313-12-51.

L´vov A.E. – Head of the Special Communications Department of the FSO of Russia. E-mail: intelteh@inteltech.ru. Tel.: +7 (812) 313-12-51.

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

Для цитирования: Мержеевский А.А., Спивак А.И., Львов А.Е. Модель построения телекоммуникационной сети специального назначения // Техника средств связи. 2021. № 2 (154). С. 31-37.

For citation: Merzheevsky A.A., Spivak A.I., L´vov A.E. Model of building a special-purpose telecommunications network. Means of Communication Equipment. 2021. No. 2 (154). Pp. 31-37 (in Russian).

АНАЛИЗ НОВЫХ ТЕХНОЛОГИЙ И ПЕРСПЕКТИВ РАЗВИТИЯ ТЕХНИКИ СРЕДСТВ СВЯЗИ

УДК 621.39

Общие принципы функционирования и требования к построению структур перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей

Будко Н.П.

Аннотация. Постановка задачи: *на основе анализа действующих технологий и существующих систем мониторинга информационно-телекоммуникационных сетей общего пользования выработать общие требования и подходы к построению перспективных систем сетевого мониторинга.* ***Цель работы:*** *обзор действующих систем мониторинга и выработка общих принципов, а также требований к построению систем сетевого мониторинга нового поколения.* ***Используемые методы:*** *методы системного анализа, структурного синтеза, технологии сетевого мониторинга Site/System Reliability Engineering, Operation Support Systems.* ***Новизна работы****: для повышения устойчивости и надежности подконтрольной сети ключевым архитектурным принципом проектирования современных подсистем мониторинга гетерогенных информационно-телекоммуникационных сетей выбран принцип распределенности и децентрализации.* ***Результат:*** *в работе определены функции подсистемы сетевого мониторинга и сервера мониторинга, как ключевого ее элемента. Предложен вариант структуры сервера мониторинга. Рассмотрены назначаемые объекты мониторинга, а также перечень собираемых с них метрических данных с точки зрения функциональной производительности сети. Сформулированы общие требования к перспективным системам сетевого мониторинга, а также общие принципы организации и функционирования подсистем мониторинга информационно-телекоммуникационной сети.*

Ключевые слова: *информационно-телекоммуникационная сеть, сервер мониторинга, техническое состояние, подсистема сетевого мониторинга, децентрализация мониторинга.*

Введение

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» и пр.), обеспечивающих пользователям предоставление различных инфокоммуникационных услуг на основе стека протоколов *TCP/IP/MPLS*, 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 (ОП) 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. 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, заключающегося в наблюдении за объектом с целью получения информации о его ТС и рабочих параметрах. На основе данных мониторинга осуществляется контроль технического состояния или остаточного ресурса объекта контроля.

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 предотвращения отказов, своевременное оповещение о них и хранение информации о ТС ИТКС и ее сетевых элементов обеспечивает актуальность данной работы. По своей сути мониторинг – это комплекс быстрого нахождения проблемы, оповещения о ней администраторов сети, а также диагностики, дающий полную и точную информацию об отказе объектов контроля (ОК) ИТКС.

Цель статьи: обзор действующих систем сетевого мониторинга и выработка на его основе общих принципов и требований к построению систем мониторинга нового поколения.

1. Учет особенностей современных ИТКС при построении их подсистем мониторинга

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*. При том, 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 системы.

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

географическая рассредоточенность ресурсов сети и источников/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;

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;

случайность функционирования ИТКС, влекущая за собой трудности при проведении анализа ее состояния (мониторинга) и организации управления;

существенная нестационарность (дрейф основных характеристик), что вызывает разную реакцию сети на одну и туже ситуацию или управление в различные моменты времени.

Сложность и актуальность создания подсистем мониторинга для таких гетерогенных ИТКС сопряжено наряду с их особенностей 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 с низким энергопотреблением, слабой вычислительной мощностью, малым объемом памяти). Указанные особенности ИТКС 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.

2. Обзор действующих систем сетевого мониторинга

Рассмотрим некоторые из существующих подсистем сетевого мониторинга.

System Center Operations Manager (*SCOM*) [12] – 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 ТС. 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 приложений в среде *Microsoft*;

обеспечение сквозного управления службами для сервисов центров обработки данных;

унифицированный контроль для частных и общедоступных облачных сервисов;

существенное повышение эффекта в управлении средой центра обработки данных;

поддержку *Windows PowerShell* 2.0 с набором новых командлетов [12].

Но одним из главных достоинств *SCOM* является продвинутая визуализация всего собранного набора метрик и представление их в виде графиков и диаграмм. При этом визуализация доступна как в специальной консоли программы, так и через веб-интерфейс.

Однако *SCOM* имеет и ряд недостатков с точки зрения решения своего функционала [12]: 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 (множестве клиентских и серверных машин в домене). Также к недостатку системы можно отнести высокую стоимость данного программного продукта.

Zabbix [13] – свободно распространяемая система для проведения комплексного мониторинга сетевого оборудования, серверов и сервисов, состоящая из следующих частей:

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 – специальная программа, запускаемая на объектах мониторинга и представляющая данные серверу по локальным ресурсам и приложениям (статистика процессора, жесткие диски, память, и т. д.) на сетевых системах. Данные системы должны работать с запущенным *Zabbix*-агентом, однако мониторинг можно осуществляться не только с помощью него, но и по *SNMP* версий 1-3, путем запуска 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. *Zabbix*-агенты поддерживаются не только на **nix* ОС, но и на *AIX* и *Windows*.

Web-интерфейс, как средство визуального представления *Zabbix*, показано на рис. 1.

Рис. 1. Вариант карты сетей в *Zabbix*

С помощью *Zabbix* обычно осуществляют распределённый мониторинг до 1000 узлов, где конфигурация младших узлов в иерархии контролируется старшими. Также продукт включает централизованный мониторинг лог-файлов. При этом имеется возможность создавать вручную по шаблону карты сетей (рис. 1), выполнять запросы в различные БД, генерировать отчёты и выявлять тенденции изменения метрик, выполнять сценарии на основе результатов мониторинга, поддерживать интеллектуальный интерфейс управления платформами (*IPMI*).

Zabbix позволяет осуществлять: автоматическое обнаружение *IP*-адресов по диапазону, доступные сервисы и производить *SNMP* проверку; автоматический мониторинг обнаруженных сетевых устройств, а также автоматическое удаление отсутствующих хостов; распределение по шаблонам и группам в зависимости от возвращаемого результата и др.

Однако, в качестве недостатков стоит отметить: громоздкость сервиса, отсутствие полной документированности возможностей и необходимость установки агантов на все машины, а также 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 [14] – свободно распространяемое программное обеспечение (ПО) под мониторинг ИТКС, изначально разработанное для ОС на базе *Linux*, но эффективно работает под *Sun Solaris, HPUX, FreeBSD, AIX*. С помощью *Nagios* доступны: мониторинг безопасности ИТКС, комплексный мониторинг за ИТ-инфраструктурой, возможность оповещать администратора сети о получаемых данных при 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*, *POP*3, *NNTP*, *ICMP*);

мониторинг состояния хостов в большинстве сетевых ОС (загрузка процессора, системные логи, использование диска);

поддержка удаленного мониторинга через шифрованные туннели *SSH* или *SSL*;

возможность построения карт сетей, рис. 2;

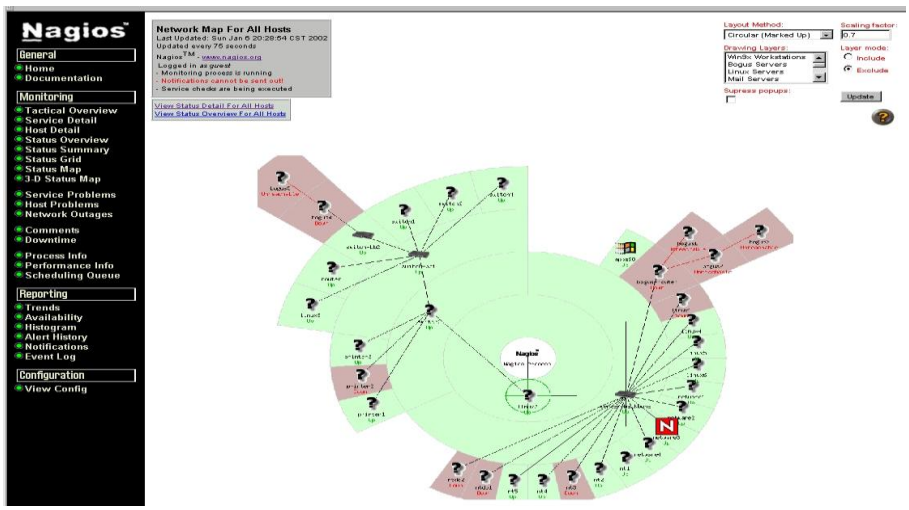


Рис. 2. Вариант карты сетей в *Nagios*

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.

К недостаткам использования *Nagios* относят «общий» характер мониторинга и его «сетевая» направленность, а также проблемы взаимодействия с серверами под ОС *Windows*.

Cacti [15] – 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 определенным критериям, причем один и тот же график может присутствовать в разных ветвях дерева или рассматриваться отдельно, с представлением временного горизонта: последний день, неделя, месяц и год (или иной временной промежуток). Имеется режим предпросмотра (просмотр заранее составленного набора графиков), рис. 3.

К достоинствам *Cacti* относят: высокую скорость развертывания при минимальном дополнительном кодировании, простоту и удобство интерфейса настройки просмотра отчетов.

Недостатками *Cacti* можно выделить: быстрое нарастание числа однотипных настроек при большом количестве сред и серверов; ограниченная производительность «неродных» *JMX* решений; невозможность инвентаризации при перераспределении ресурсов и модернизации.

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, в то время как попытки мониторинга нестандартных метрик значительно снижают производительность программного продукта.

Prometheus – свободно распространяемое ПО в интересах мониторинга сетевых устройств, серверов и сервисов, имеет встроенный базовый сетевой интерфейс (рис. 4), но чаще используется в связке с сервером визуализации данных ***Grafana*** (рис. 5) В ее состав входят:

Сервер мониторинга, который выполняет периодический опрос и сбор данных, а также их обработку и анализ. В случае обнаружения аномалии осуществляется 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). В качестве недостатка стоит отметить, 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 большое множество экспортеров предназначенных как для сбора метрик из всех видов ОС, так и для сбора метрик из конкретных программных продуктов. При необходимости кастомизации может быть дописан самостоятельно или переписан для реализации отправки метрик элементу *Pushgateway*. Предоставляет *web*-интерфейс для доступа к метрикам объекта мониторинга, который опрашивается сервером мониторинга.

Pushgateway – специальное программное обеспечение, 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.

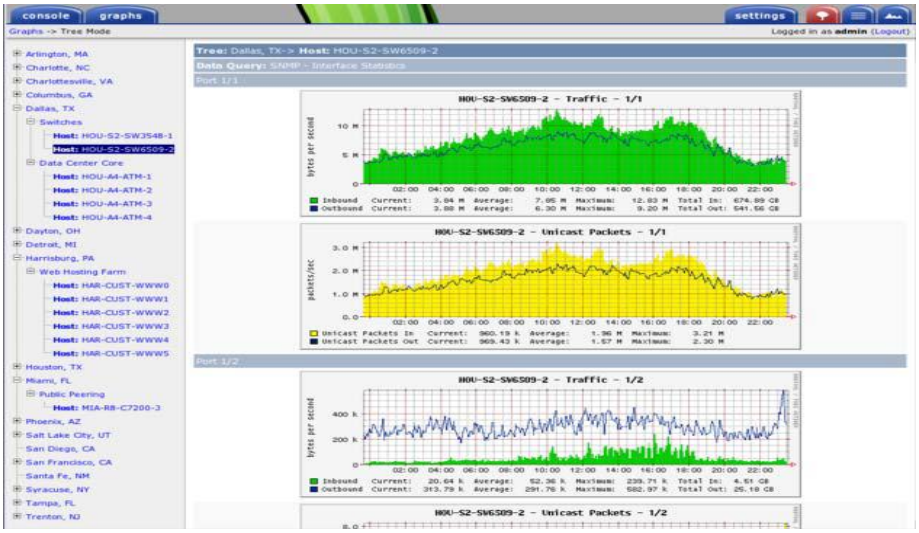


Рис. 3. Интерфейс *Cacti* [15]

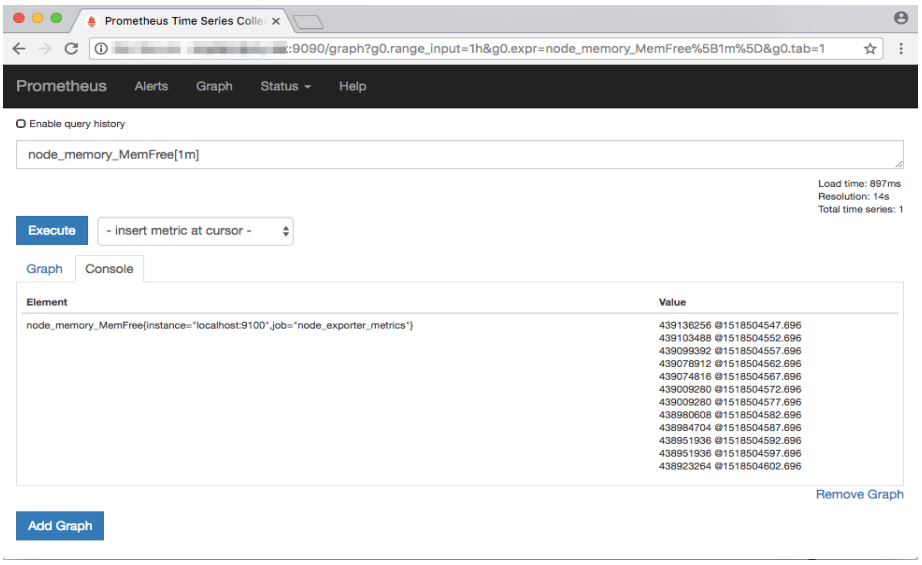


Рис. 4. *Web*-интерфейс системы мониторинга *Prometheus*

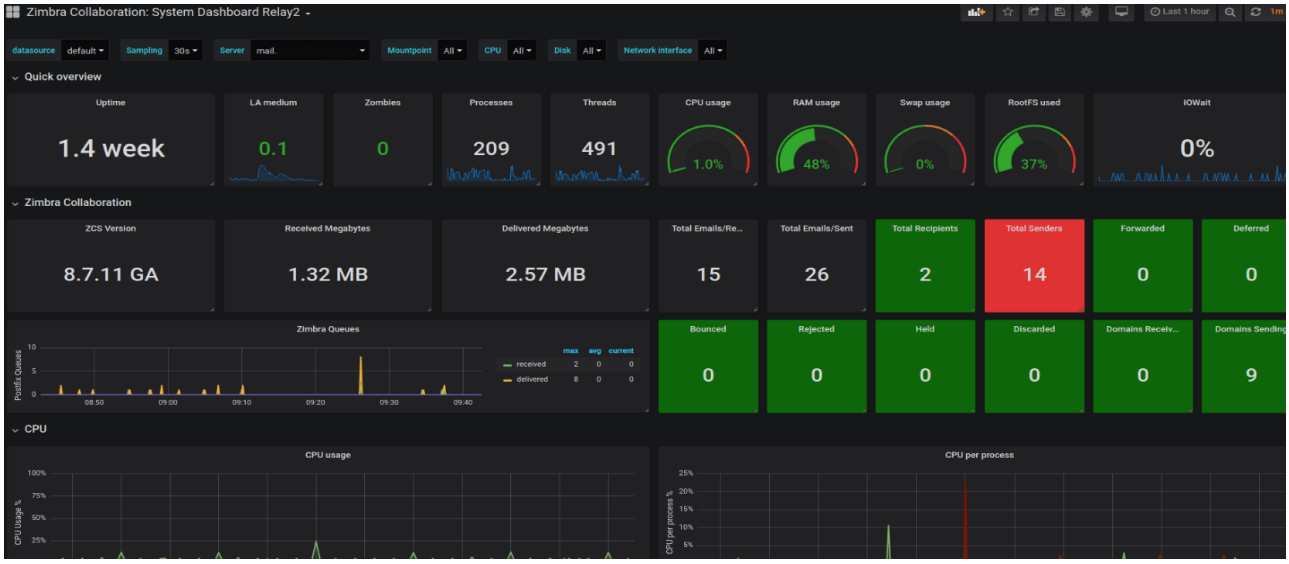


Рис. 5. *Web*-интерфейс сервера визуализации данных *Grafana*

Operation Support Systems (*OSS*) [16] – системы поддержки операций, построенные на базе протокола *SNMP v.* 1 и 2. Используются ведущими телекоммуникационными компаниями.

В рассматриваемой высокоуровневой архитектуре *OSS Hewlett-Packard (HP) OpenView-NNM, OpenNMS*, а также *Huawei U2000LCT* (рис. 6), центральным компонентом *OSS* является компонент диспетчеризации событий, совмещенный с настраиваемым классификатором событий, отказов и предупреждений (рекомендация М.3703 [17]). 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*).

В рассматриваемых *OSS* можно выделить 3-уровневую схему обработки [17]: данные (*date*), получаемые посредством измерений; события (*events*), получаемые после обработки процессами сбора первичных данных при сравнении метрики с пороговым значением; отказы (*faults*) и предупреждения (*alarms*), получаемые в результате логического вывода на множестве событий (*events*). В процессе обработки наблюдается сокращение 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 [17].

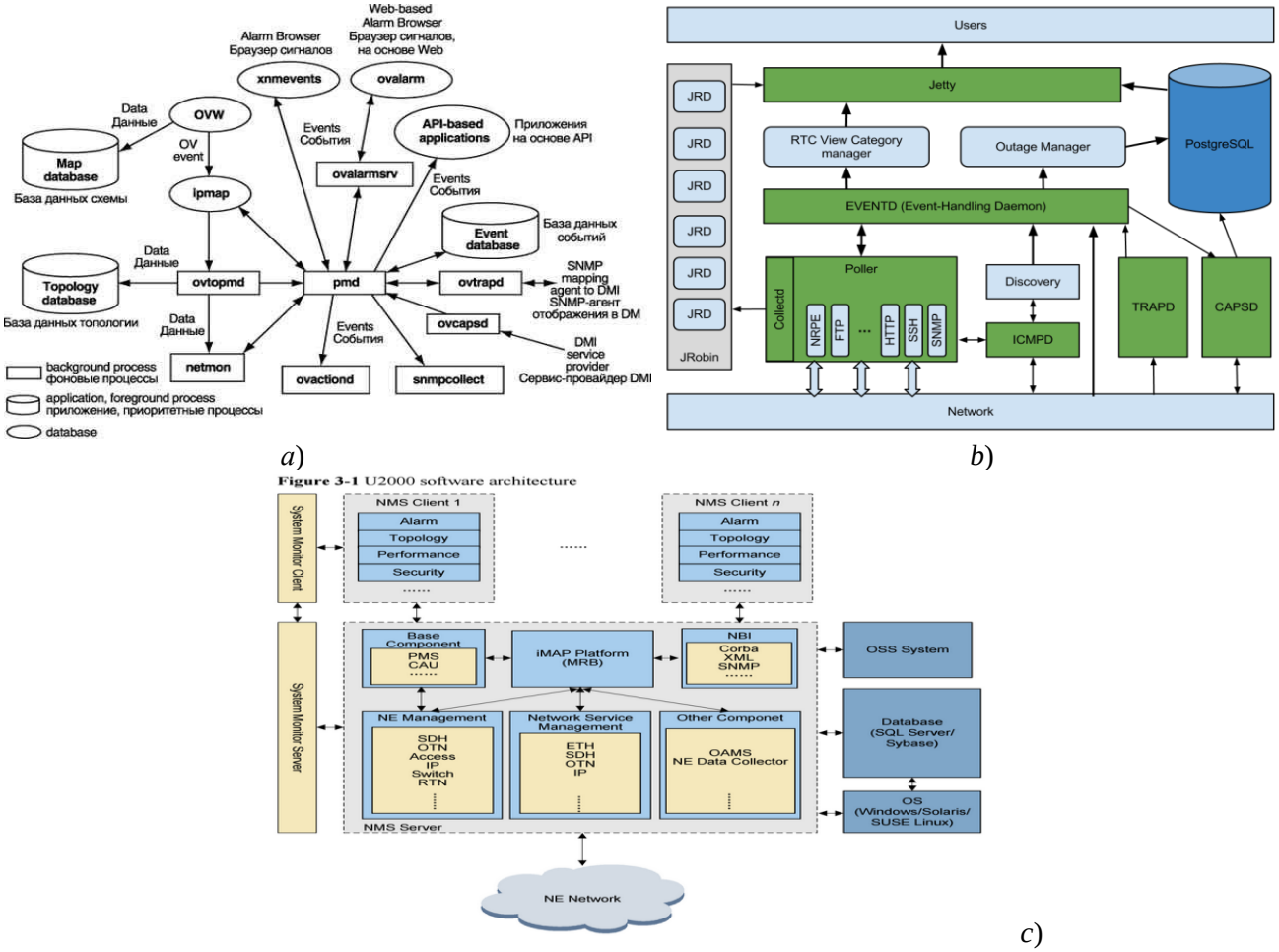


Рис. 6. Высокоуровневые архитектуры (*a*) *Hewlett-Packard NNM* [16], (*b*) *OpenNMS* и (*c*) *U2000LCT Huawei* [16]. Интеграция за счет компонента-диспетчера классифицированных событий

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. Поля условно делят на часть, относящуюся к объекту управления – (устройству) и субъекту управления (агенту или компоненту), производящему операции над сетевым элементом в системе управления (СУ). В ходе обработки событие может передаваться по цепочке субъектов *«устройство» – «агент» – «компонент сбора данных» – «компонент диагностики»* [17], т. е. в процессе обработки событий субъекты выстраиваются в цепочки.

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

К примеру, индикаторами доступности *SRE* являются следующие метрики времени:

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 [20]:

RPO (*Recovery Point Objective*) – максимальный период времени, за который могут быть потеряны данные в результате инцидента (целевая временн*а*я точка восстановления ИТКС). Для телеком-оператора данный показатель необходимо минимизировать, и, в идеале, свести к нулю, $RPO \rightarrow 0$. 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 [19], 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-инфраструктуры, 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 *IT*-сервиса: доступность (*availability*); производительность (*performance*); надежность (*reliability*); сопровождаемость (*maintainability*); обслуживаемость (*serviceability*); безопасность (*security*) [21]. 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 [22].

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 ее размещения.

Территориальное ограничение применения систем мониторинга *SLA* в ИТКС не должно рассматриваться как уменьшение их значимости. Эти средства контроля применяются только в точках демаркации на границах подсетей, но в настоящее время количество таких точек растет с увеличением номенклатуры систем, сервисов, различного оборудования и др. При этом область квалиметрии и метрологии в точках демаркации, наоборот, расширяется по мере развития ИТ. Причем 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 [23] (рис. 7): оператор-оператор – точка при взаимодействии операторов; оператор-пользователь – точка подключения клиента; 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*).

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 конвенции *SLA*.

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. В том случае, если речь идет о новой технологии, для которой еще нет разработанных норм национальных стандартов, и присутствует правовой вакуум, *SLA* – единственный способ урегулирования взаимоотношений.

Рис. 7. Варианты точек демаркации [23]

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 жизненного цикла услуги (*PLM*), рис. 8.

Рис. 8. Сквозной цикл предоставления услуги в соответствие со *SLA*-контрактом

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, стандартами и политикой качества компании-оператора [24]). Все это делает системы мониторинга *SLA* весьма актуальными и значимыми, относя их к классу самых современных. Ориентированность на обеспечение процесса делает эти системы мониторинга результативными, что в сочетании с оперативностью развёртывания и технологичностью, усиливает эффективность данного класса систем на рынке ИТ России.

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. Только 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. Причем, 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 [25]. 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 параметров 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. Рассмотрим их:

Amazon CloudWatch [26] – это служба мониторинга и управления, отслеживающая виртуальные ресурсы пользователей, такие как экземпляры виртуальных машин *Amazon EC*2;

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] и ***HP Open View*** [30] – другие системы мониторинга, направленные 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.

3. Функции подсистемы мониторинга информационно-телекоммуникационной сети

Изначально на ИТКС 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 ОК были привязаны к практическому опыту работы конкретного специалиста с сетевой инфраструктурой и полностью терялись при его увольнении. В настоящее время 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 (СУБД), 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. 9.

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 за одним и тем же объектом на протяжении заданного времени наблюдений. Таким образом, возможно определение изменений значений параметров объекта во времени.

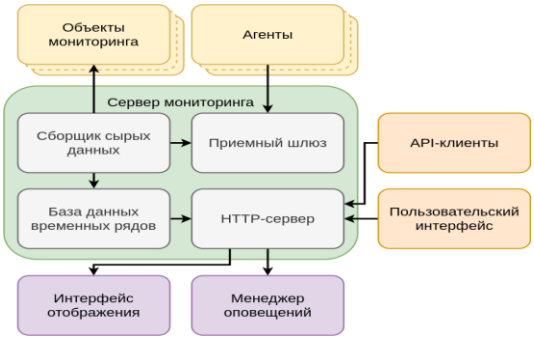


Рис. 9. Структурная схема сервера мониторинга ИТКС ОП и зависимых элементов (*вариант*)

Сервер мониторинга функционально предназначен для решения следующих задач:

сбор ИИ о ТС элементов ИТКС (сетевых устройствах, функционирующем на них ПО и пр.);

обработки, обобщения, хранения и отображения информации о состоянии элементов;

изменения числа объектов мониторинга через графический интерфейс пользователя;

графического и табличного отображения данных (в т. ч. отображения динамики изменения контролируемых параметров в течение установленного временного интервала);

оповещения должностных лиц (ДЛ) о возникновении критических событий в системе;

автоматического или автоматизированного реагирования на возникновение критических событий (в соответствии с заранее настроенной логикой);

ведения системных журналов: изменения состояния сетевых элементов и их отдельных параметров, действий системы и действий пользователя, изменения параметров системы.

При выборе, разработке (построении) и внедрении систем мониторинга сначала необходимо определиться с объектами, которые будут подвергаться контролю, а также выбрать показатели качества и критерии эффективности (наступления критических событий), которые и определят количество оповещений при отказе (сбое), частоту сканирования и другие параметры, а также последствия для ИТКС. Обычно на больших сетевых инфраструктурах перед финальным внедрением подсистем мониторинга разворачивают тестовый сегмент сети в виде стенда, на котором возможно оценить целесообразность принятых решений при определении пороговых значений на контролируемые параметры, проанализировать «узкие места» в ИТКС.

К *объектам мониторинга* локальной вычислительной сети (ЛВС) можно отнести следующие программные и технические средства: автоматизированные рабочие места (АРМ) ДЛ; серверное оборудование; специализированное оборудование; сервер печати; систему единого времени; комплекс средств защиты информации. Для региональных и глобальных ИТКС перечень оборудования, соответственно будет значительно шире.

С точки зрения функциональной производительности ИТКС подсистема мониторинга должна осуществлять сбор следующих данных о вычислительных ресурсах объекта мониторинга:

тактовая частота процессора;

объем свободной оперативной памяти;

свободный и использованный объем жесткого диска;

количество переданных, потерянных пакетов и коллизий сетевых интерфейсов;

сбор сведений из системных журналов стороннего программного обеспечения;

сбор сведений о запущенных процессах;

отправка данных в инициативном порядке и по запросу в активном и пассивном режимах;

интерфейс управления встроенными командами и оборудованием по протоколу *SSH*.

Посредством использования протокола *SNMP* сервер мониторинга через сборщик сырых данных осуществляет сбор следующих *метрических данных* сетевого устройства, обеспеченного поддержкой протокола обмена информацией *SNMP*:

статус порта: есть физическое подключение или нет, включен/выключен – программно;

время последнего изменения настроек порта;

размер наибольшего пакета, который может быть отправлен с устройства;

скорость порта;

список *VLAN* (для коммутаторов ЛВС);
время работы устройства;
описание устройства;
средняя загрузка процессора за 5 с, за 1 мин, за 5 мин;
причина перезагрузки;
описание и состояние датчиков температуры;
объем свободной оперативной памяти;
список *IP*-адресов интерфейсов;
таблица маршрутов для маршрутизаторов;
входящий и исходящий трафик;
счетчик принятых и счетчик отправленных *Unicast* пакетов;
счетчик принятых и счетчик отправленных *Broadcast* пакетов;
счетчик принятых и счетчик отправленных *Multicast* пакетов;
счетчик принятых пакетов с ошибками и счетчик отправленных пакетов с ошибками;
счетчик отброшенных пакетов, которые не содержали ошибок, но были отброшены, например, для освобождения буферного пространства.

Перечень собираемых метрических данных по различным ОК может отличаться.

Собранные сборщиком сырых метрических данных направляются в сервер мониторинга для обработки информации и предоставления отчетов в виде таблиц и графиков с возможностью экспорта в форматы *CSV*, *PDF*, *XML*, *PNG* в интересах ДЛ. Характер метрических данных, необходимых к сбору, уточняется и устанавливается функциональным ДЛ (администратором).

Среди ***основных функций*** подсистемы мониторинга ИТКС выделим 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 ИИ ДЛ, 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 существующих систем сетевого мониторинга определим основные функции сервера мониторинга *перспективной подсистемы мониторинга* ИТКС, к основным из которых можно отнести функции выборки, назначения, *ping* и *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 и т. д.).

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. К примеру, каждый сервер мониторинга может начать случайный выбор узлов, за которыми еще не ведется наблюдение, и назначить их себе.

3) *Функция проверки связи (ping).* Целью функции проверки связи является выполнение проверки связи с сетевыми устройствами, назначенными серверу мониторинга, и записать результаты 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 сети (с помощью 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 SNMP*. 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. Агрегированные данные хранятся в экземпляре распределенной БД. Репликация данных между всеми экземплярами гарантирует, что новые данные автоматически реплицируются и распределяются по всем экземплярам БД, обеспечивая выполнение технологии *CRDT**.

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.

4. Требования к перспективным системам сетевого мониторинга

Современные системы мониторинга, чтобы оставаться востребованными на рынке телекоммуникационных услуг проходят наряду с сетевыми устройствами и технологиями постоянный процесс совершенствования и модернизации. Это в свою очередь влияет на изменение требований к системам мониторинга в сторону их ужесточения. В настоящее время выделяют следующие требования к новым системам мониторинга, внедряемым на ИТКС [33]:

резервирование: каждое сетевое устройство должно контролироваться произвольным минимальным количеством серверов, например, превышающим один. Это означает, что серверы мониторинга должны проверять, какие сетевые устройства имеют назначенные серверы мониторинга, и, если их количество ниже минимального (менее двух), самостоятельно принимать решение стать сервером мониторинга для любого из этих устройств;

**CRDT* (*Conflict-Free Replicated Data Type*) – типы данных, которые можно реплицировать на много узлов и обновлять параллельно без координации между узлами.

автоматическое распределение: система автоматически выполняет распределение между сетевыми устройствами и серверами мониторинга. При постоянной работе служба должна работать автономно без ручного вмешательства;

автоматическая реконфигурация: система должна иметь возможность автоматически обнаруживать неисправные серверы мониторинга (например, из-за сбоев сети или оборудования) и переназначать сетевые устройства функциональным серверам мониторинга. Этот процесс должен выполняться без ручного вмешательства;

репликация данных: собранные данные должны быть реплицированы и распределены по разным частям системы. В случае разделения сети или деградации БД данные по-прежнему должны быть доступны для извлечения службой мониторинга из других сегментов сети;

балансировка нагрузки: рабочая нагрузка мониторинга должна быть распределена по сети и активным серверам мониторинга, а не концентрироваться на нескольких устройствах.

Сравнение перспективных и существующих систем мониторинга приведено в табл. 1.

Таблица 1 – Сравнение перспективных и существующих систем сетевого мониторинга

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

5. Общие принципы организации и функционирования подсистем мониторинга ИТКС

На основе системного анализа процессов мониторинга ИТКС, проведенного выше, сформулируем общие принципы построения и функционирования систем сетевого мониторинга.

Для решения задач поддержания в постоянной готовности к применению и обеспечения эффективной технической эксплуатации сетевых элементов и ИТКС в целом, необходимо применение современной организационно-технической идеологии и подходов к построению систем сетевого мониторинга, основанной на использовании перспективных интеллектуальных, информационных, сетевых и измерительных технологий. При этом функционал подсистемы мониторинга территориально распределенной ИТКС должен включать комплекс мероприятий, проводимых, с целью информационного обеспечения СППР (по управлению связью – АСУС) и поддержания сетевых элементов в исправном (работоспособном) состоянии. Исходя из этого, основными принципами построения подсистемы мониторинга ИТКС являются:

принцип эволюционного развития, предоставляющий возможность подсистеме мониторинга соответствовать постоянно совершенствующимся (эволюционирующим) ИТКС, с учетом их топологической и пространственно-временной неоднородности;

единства организационно-технических, алгоритмических и программно-технических решений, направленных на разработку высокоэффективных программных приложений по

поддержанию и восстановлению качества функционирования ИТКС и ее сетевых элементов на основе данных мониторинга;

интеллектуализации процессов мониторинга ИТКС, базирующийся на применении перспективных ИТ, развивающихся на стыке искусственного интеллекта и распределенной обработки больших данных (измерительной информации сетевых элементов);

гибкости архитектуры подсистемы мониторинга на основе методологии открытых систем, обеспечивающей возможность реконфигурации системы контроля в условиях деградации и восстановления сетевой инфраструктуры, а также наращивания функций мониторинга ИТКС и ее сетевых элементов – многоуровневость, иерархическое построение.

Но основными архитектурными принципами проектирования современных подсистем мониторинга распределенных гетерогенных ИТКС являются *распределение* и *децентрализация* для повышения устойчивости и надежности подконтрольной сети. Остановимся на них подробно.

Механизм децентрализованного распределения успешно обеспечивает установку минимального количества серверов мониторинга на одно контролируемое сетевое устройство, что удовлетворяет заданным системным требованиям. Учитывая, что на распределенной ИТКС обстановка по связи постоянно изменяется из-за динамичной смены состояния каналов связи и надежности сетевых элементов для повышения отказоустойчивости подсистемы мониторинга предлагается каждому сетевому элементу сопоставлять несколько серверов мониторинга, находящихся на границах подсетей (сегментов сети). При этом принцип распределенности и децентрализации предполагает размещение на сети нескольких реплик серверов мониторинга.

Проведенный выше анализ особенностей развития современных ИТКС и этапов их совершенствования показал экспоненциальный рост структур [32], порождаемый увеличением географической распределенности, а также возрастанием уровня разнородности сегментов сети, что в свою очередь накладывает особенности на подходы и методы построения структур их подсистем мониторинга. Причем, большая степень размерности контролируемого пространства, с учетом многоуровневой структуры и гетерогенности ИТКС, совокупности наблюдаемых метрик на сетевых элементах, представляющих из себя большие данные (*Big Data*), предполагает разработку модели системы, способной учесть вышеизложенные требования, предъявляемые к перспективным системам мониторинга. Основным из них является *децентрализация инфраструктуры мониторинга* функционального состояния распределенных сетевых ресурсов .

6. Структура перспективной подсистемы мониторинга ИТКС общего пользования

Структуру подсистемы мониторинга такой распределенной гетерогенной ИТКС можно смоделировать как неполным двунаправленным графом $G = (N, E)$, где N – это набор узлов, составляющих сеть, а E – набор связей (беспроводных или оптоволоконных), соединяющих корреспондирующие пары узлов. Изолированные узлы сети (т. е. без связей с другими узлами) отбрасываются. При этом для построения подсистемы мониторинга рассмотрим два типа узлов: серверы мониторинга M ($M \in N$) и сетевые устройства, подлежащие мониторингу D ($D \subset N$). Связи характеризуются заданной пропускной способностью V_{ij}, $\forall (i, j) \in E$ и задержкой T_{ij}, $\forall (i, j) \in E$, в то время как каждый i-й узел имеет конкретное качество мониторинга (при рассмотрении мониторинга как услуги) QoS_i, $\forall\ i \in N$, полученное из реальных измерений на сети. Для развертывания подсистемы мониторинга на сети можно разместить не более $M_{\max} = k$ реплик сервера мониторинга. Сервер мониторинга может быть развернут в сетевом узле, только если этот узел имеет QoS_i выше минимального порога, $QoS_i > QoS_{min}$ [23]. Ссылка узла будет использоваться, если его полоса пропускания выше или равна заданному порогу. При сопоставлении сетевых устройств и серверов мониторинга учтем следующее ограничения (оно м. б. установлено и иным, в зависимости от важности выполняемых функций, включения в КВИ):

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

Поскольку основными принципами проектирования подсистемы мониторинга являются *распределение* и *децентрализация* для повышения устойчивости и надежности, то необходимо использовать распределенные структуры БД для поддержки децентрализованной координации

серверов мониторинга. С этой целью серверы должны хранить распределенное сопоставление серверов мониторинга и сетевых устройств, используемое для динамического взятия (и снятия) устройств на мониторинг. Такое динамическое распределение должно модифицироваться одновременно любым из участвующих серверов для поддержки выполнения условия (1). Чтобы обеспечить это, используем технологию *CRDT* и делегируем синхронизацию данных, а также их согласованность, на базовый уровень хранения (БД), который обеспечивает определенные свойства (например, гарантированную конечную согласованность при репликации данных).

Распределенное сопоставление на ИТКС серверов мониторинга и сетевых устройств приведено на рис. 10 и в табл. 2. В данной сетевой инфраструктуре группа маршрутизаторов *D*1 – *D*12 представляют фактические сетевые устройства, соединенные между собой оптоволоконными либо радиоканалами и образующие ячеистую сеть. Вокруг них показаны сервера мониторинга *M*1 – *M*6, взаимодействующие друг с другом для обмена информацией (репликации мониторинговой информации) и координации своих действий.

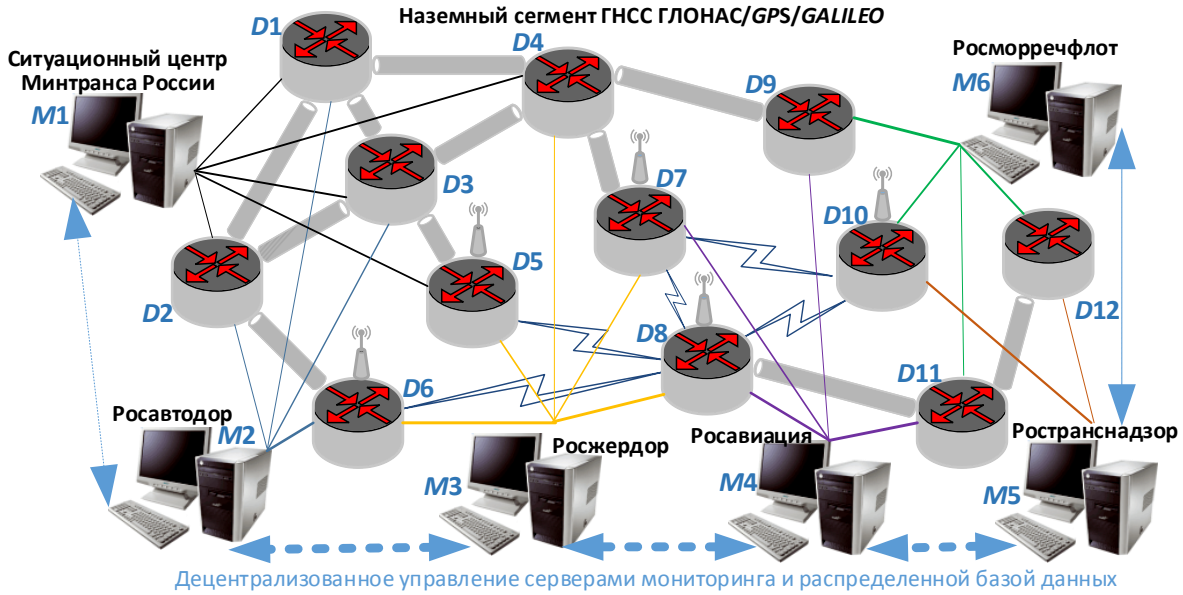


Рис. 10. Децентрализованная система сетевого мониторинга (*вариант на примере Минтранса России*)

Таблица 2 – Распределенное сопоставление серверов мониторинга и сетевых устройств (по рис. 10)

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

Структура, приведенная на рис. 10 может соответствовать межведомственной ИТКС, осуществляющей мониторинг состояния единого дифференциального сервиса Глобальной навигационной спутниковой системы (ГНСС) ГЛОНАС/*GPS*/*GALILEO* при его использовании в Министерстве транспорта РФ в интересах сегментов ИТКС Федеральных Агентств Росавтодора, Росжелдора, Росавиации, Росморречфлота и Ространснадзора для управления движением поездов (ДП), автомобильным транспортом (АПК «Умный город»), систем связи и радиотехнического обеспечения при организации системы управления воздушным движением (ВД), систем автоматизированного управления (АСУ) движением судов (ДС) на внутренних водных путях (ВВП) и в морских акваториях. При этом сервера мониторинга размещаются как на телекоммуникационных структурах автомобильных и железных дорог, районов воздушного движения и районных администраций бассейнов рек (озер), до единых центров управления (ЕЦУ) ДП, ЕЦУ ВД, ЕЦУ ДС, так и в ситуационном центре (СЦ) Минтранса РФ.

Заключение

В статье представлен обзор действующих технологий и систем сетевого мониторинга ИТКС ОП. Дана характеристика таким из них как *SCOM, Zabbix, Nagios, Cacti, OSS, SRE, SLA, Amazon CloudWatch, IBM Tivoli Monitoring, GMonE, PCMONS* 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. При этом для повышения устойчивости и надежности подконтрольной сети ключевым архитектурным принципом проектирования современных подсистем мониторинга распределенных гетерогенных ИТКС определен принцип *распределенности и децентрализации*.

На основе предложенных принципов построена структура перспективной подсистемы мониторинга ИТКС ОП на примере Минтранса РФ. В ней в соответствии с требованиями, изложенными в статье, каждому сетевому элементу назначают два и более сервера мониторинга, каждый из которых географически разнесен, имеет разную емкость и доступные ресурсы, некоторые из них отвечают за мониторинг б*о*льшего количества сетевых устройств, чем другие.

Важным элементом заявленной структуры подсистемы мониторинга является предлагаемое сопоставление сетевых элементов серверам мониторинга, разработанное как совместно используемый объект распределенных данных, который не управляется централизованно, а динамически обновляется децентрализованно и автономно самими серверами мониторинга с делегированием синхронизации и согласованности данных на базовый уровень хранения данных, который обеспечивает определенные свойства (например, гарантированную конечную согласованность при репликации данных). В конструкции системы мониторинга применяется децентрализованная координация между серверами мониторинга. Каждый из них считывает мгновенное состояние корреспондирующих серверов мониторинга для управления своими индивидуальными действиями (настройками) по отношению к сетевым элементам (какие устройства контролировать). Это решение затем запускает фактическую операцию мониторинга, которая проводится, как и в традиционной централизованной системе.

Алгоритм децентрализованного распределения успешно обеспечивает установку минимального количества серверов мониторинга ($M \geq 2$) на одно сетевое устройство, что удовлетворяет установленным системным требованиям. Такая устойчивая и децентрализованная архитектура может заложить основу для других приложений в области облачных пограничных вычислений, которым важно координировать распределенные и согласованные общие данные. При этом БД используется *CRDT*-технология, реализующая структуры распределенных данных.

Литература

1. Инфокоммуникационные сети: энциклопедия. Кн. 4. Гетерогенные сети связи: принципы построения, методы синтеза, эффективность, цена, качество / П. А. Будко, И. А. Кулешов, В. И. Курносов, В. И. Мирошников; 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: 30.04.2021).

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 (дата обращения: 30.04.2021).

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 (ред. 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. TechNet Magazine: System Center Operations Manager 2012: Простота расширения возможностей мониторинга. – URL: http://technet.microsoft.com (дата обращения 03.05.2021).

13. Vacche A. D., Lee S. K. Zabbix Mastering. Packt Publ., 2013. 358 p. (дата обращения 24.04.2021).

14. Nagios: отраслевой стандарт мониторинга ИТ-инфраструктуры. – URL: https://www.nagios.org/, 2019. (дата обращения 03.05.2021).

15. XGU [Электронный ресурс]: Cacti. – URL: http://xgu.ru (дата обращения 03.05.2021).

16. 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.

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

18. Бломмерс Дж. OpenView Network Node Manager: Разработка и реализация корпоративного решения. – М.: Интернет Ун-т Информационных Технологий, 2005. – 264 с.

19. https://www.osp.ru/itsm/2012/09/13017362.html (дата обращения 21.03.2021).

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. https://olontsev.ru/2016/04/rpo and rto/ (дата обращения 21.03.2021).

22. https://ru.wikipedia.org/wiki/Соглашение_об_уровне_услуг (дата обращения 21.03.2021).

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

24. Будко П. А., Линец Г. И., Мухин А. В., Фомин Л. А. Эффективность, цена и качество информационно-телекоммуникационных систем. Методы оптимизации: Монография. – СПб.: ВАС, 2011. – 420 с.

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

26. Amazon, «Amazon CloudWatch». – URL: https: //aws.amazon.com/cloudwatch (дата обращения 03.05.2021).

27. Montes H., Sanchez A., Memishi B., Perez M. S., Antόnio G. Gmone: an integrated approach to cloud monitoring. Future Generation Computer Systems, 2013, vol. 29, no. 8, pp. 2026-2040 (дата обращения 03.05.2021).

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 03.05.2021).

30. HP BTO OpenView. – URL: http://www.hp.com/hpinfo/newsroom/press_kits/2010/HPSoftwareUniverseBarcelona2010/HP_Applications_ Portfolio_brochure.pdf, 2019 (дата обращения 03.05.2021).

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. Каретников В. В., Будко Н. П., Аллакин В. В. Синтез подсистемы интеллектуального мониторинга информационно-телекоммуникационной сети в интересах информационного обеспечения ситуационного центра Минтранса России // Вестник Астраханского государственного технического университета. Серия: управление, вычислительная техника и информатика. 2021. № 2. С. 64-81.

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

References

1. Budko P. A., Kuleshov I. A., Kurnosov V. I., Miroshnikov V. I. *Infokommunikatsionnyye setiю Entsiklopediya. Kniga 4. Geterogennyye seti svyazi. Printsipy postroyeniya. Metody sinteza. Effektivnost. Tsena. Kachestvo. Monografija* [Infocommunication networks: an encyclopedia. Book 4. Heterogeneous communication networks. Principles of construction. Methods of synthesis. Efficiency. Price. Quality. Monography]. 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. –URL: https://www.itu.int/rec/T-REC-Y.2011-200410-I/en (accessed 30 April 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, UK. 2017 (accessed 30.04.2021).

4. Budko P. A. *Upravleniye resursami informatsionno-telekommunikatsionnykh sistem. Metody optimizatsii* [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. *K voprosu obosnovaniya ponyatiynogo apparata nerazrushayushchego ekspress-kontrolya tekhnicheskogo sostoyaniya oborudovaniya sistemy svyazi i radiotekhnicheskogo obespecheniya aerodrome* [To the question of substantiation of the conceptual apparatus nondestructive express control of the technical condition equipment of the communication system and aerodrome radio engineering support]. H&ES Research, 2019, v. 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]. Under the general editorship of V. V. Klyuev. Moscow, Mechanical Engineering, 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: Monografiya* [Multilevel synthesis of information and telecommunications systems. Mathematical models and optimization methods: A monograph]. Saint-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. TechNet Magazine: System Center Operations Manager 2012: Ease of expanding monitoring capabilities. – URL: http://technet.microsoft.com (accessed 03 May 2021).

13. Vacche A. D., Lee S. K. Zabbix Mastering. Packt Publ. Ltd, 2013. 358 p. (accessed 24 April 2021).

14. Nagios: Industry Standard for Monitoring IT Infrastructure. URL: https://www.nagios.org/2019. (accessed 03 May 2021).

15. XGU: Cacti. URL: http://xgu.ru (accessed 03 May 2021).

16. Vasiliev N. V., Rakov I. V., Zabrodin O. V., Kulikov D. V. *Analytical and synthetic OSS: analysis of approaches and methods* [Analytical and synthetic OSS: analysis of approaches and methods] Means of Communication Equipment. 2019, no. 1 (145), pp. 82-94. (in Russian).

17. 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 (accessed 03 May 2021).

18. Blommers J. OpenView Network Node Manager: Designing and Implementing an Enterprise Solution. Moscow, "INTUIT.RU", 2005. 264 p. (in Russian).

19. https://www.osp.ru/itsm/2012/09/13017362.html (accessed 21 Mart 2021).

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 (151), pp. 77-85. (in Russian).

21. https://olontsev.ru/2016/04/rpo and rto (accessed 21 Mart 2021).

22. https://ru.wikipedia.org/wiki/ Service Level Convention (accessed 21 Mart 2021).

23. Baklanov I. G. Justification of OSS. Moscow. Publishing solutions Publ., 2016. 131 p. (in Russian).

24. Budko P. A., Linets G. I., Mukhin A.V., Fomin L. A. *Effektivnost', tsena i kachestvo informatsionno-telekommunikatsionnykh sistem. Metody optimizatsii: Monografiya* [Efficiency, price and quality of information and telecommunications systems. Optimization methods: Monograph]. Saint-Petersburg, Military Academy of Communications Publ., 2011, 420 p.

25. Storozhuk M. *Ispol'zovaniye sistem monitoringa setey dlya obespecheniya raboty kriticheski vazhnykh prilozheniy* [Using Network Monitoring Systems to Keep the Critical Applications Running]. Last Mile, 2021, no 1, pp. 40-44. (in Russian).

26. Amazon, «Amazon CloudWatch», https: //aws.amazon.com/cloudwatch (accessed 03 May 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 03.05.2021).

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.

98. IBM, «IBM Tivoli Monitoring», https://www.ibm.com/support/knowledgecenter/en/SS3JRN7.2.0 /com.ibm.itm.doc/itminstall06.htm (accessed 03 May 2021).

30. HP, «HP BTO OpenView», http://www.hp.com/hpinfo/newsroom/ press_kits / 2010 / HPSoftware UniverseBarcelona2010 / HP_Applications_ Portfolio_brochure.pdf, 2019 (accessed 03 May 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. Karetnikov V. V., Budko N. P., Allakin V. V. Synthesis of subsystem of intelligent monitoring of information and telecommunication network of departmental situational center. Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics. 2021;3:64-81. (In Russian.) DOI: 10.24143/2072-9502-2021-3-64-81.

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

Статья поступила 22 апреля 2021 г.

Информация об авторе

Будко Никита Павлович – Соискатель ученой степени кандидата технических наук. Независимый специалист. E-mail: budko62@mail.ru. Адрес: 194064, г. Санкт-Петербург, ул. Бутлерова, 9, корп. 1, кв. 252.

General principles of functioning and requirements for the construction of structures of promising monitoring systems for distributed information and telecommunications networks

N.P. Budko

Annotation. Task statement: *based on the analysis of existing technologies and existing monitoring systems of public information and telecommunications networks, to develop general requirements and approaches to the construction of promising network monitoring systems.* ***The purpose of the work:*** *to review the existing monitoring systems and develop general principles and requirements for the construction of a new generation of network monitoring systems.* ***Methods used:*** *methods of system analysis, structural synthesis, network monitoring technologies Site/System Reliability Engineering, Operation Support Systems.* ***The novelty of the work:*** *to increase the stability and reliability of the controlled network, the key architectural principle of*

designing modern monitoring subsystems of heterogeneous information and telecommunications networks is the principle of distribution and decentralization. ***Result:*** *the paper defines the functions of the network monitoring subsystem and the monitoring server as its key element. A variant of the monitoring server structure is proposed. The assigned monitoring objects are considered, as well as a list of metric data collected from them from the point of view of the functional performance of the network. General requirements for prospective network monitoring systems are formulated, as well as general principles of organization and functioning of information and telecommunications network monitoring subsystems.*

Keywords: *information and telecommunications network, technical condition, network monitoring subsystem, monitoring server, decentralization of monitoring infrastructure.*

Information about Author

Budko Nikita Pavlovich – Doctoral Student. Independent Expert. E-mail: budko62@mail.ru. Address: 194064, Russia, St. Petersburg, Butlerova str., build. 9/3, sq. 252.

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

For citation: Budko N.P. General principles of functioning and requirements for the construction of structures of promising monitoring systems for distributed information and telecommunications networks. Means of Communication Equipment. 2021. No. 2 (154). Pp. 38-60 (in Russian).

УДК 621.39

Анализ методов оценки временных рядов сервером мониторинга информационно-телекоммуникационной сети общего пользования

Аллакин В.В.

Аннотация. Постановка задачи: *на основе анализа научно-методического аппарата оценки временных рядов наблюдаемых метрик выработать подход к формированию методики прогнозирования (превентивной идентификации) аномальных ситуаций по результатам мониторинга функционального состояния сетевых элементов информационно-телекоммуникационных сетей общего пользования.* ***Цель работы****: разработка алгоритма методики идентификации аномальных ситуаций сервером мониторинга по наблюдаемым временным рядам метрик сетевых элементов.* ***Используемые методы****: методы теории анализа, теории прогноза, теории надежности, теории диагностики, теории классификации, методы кластерного анализа, топологические методы анализа временных рядов, методы поведенческой аналитики, символьное представление временных рядов.* ***Новизна****: превентивная идентификация аномального состояния сетевого элемента путем выявления «запрещенных» кодовых комбинаций при наблюдении временных рядов, 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 технического состояния 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.* ***Результаты****: проведен анализ научно-методического аппарата решения задач прогноза временных рядов, в результате чего для достижения поставленной цели исследования выбран метод символического представления временных рядов, на основе 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 кодирования временных рядов, этапа идентификации вида технического состояния сетевого элемента и завершающего.* ***Практическая значимость****: анализ методов оценки временных рядов позволил выработать подход к построению алгоритма функционирования сервера мониторинга для идентификации аномалий в работе информационно-телекоммуникационной сети общего пользования.*

Ключевые слова*: сервер мониторинга, временной ряд, прогнозирование аномальной ситуации, превентивная идентификация вида технического состояния, особый режим мониторинга.*

Введение

Изменение большого числа контролируемых характеристик информационно-телекоммуникационных сетей (ИТКС) общего пользования (ОП) и ее основных элементов (серверов, узлов коммутации, периферийных устройств, каналов передачи данных) 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 его опроса серверами мониторинга, что существенно влияет на увеличение количества обрабатываемой измерительной информации (ИИ) сервером мониторинга. А учитывая тот факт, что наблюдение за сетевыми объектами мониторинга осуществляется практически на протяжении всего их жизненного цикла, то задачи обработки временных рядов в современных подсистемах мониторинга справедливо относят к задачам анализа больших данных (*Big Data*).

Временной ряд показателей надежностных характеристик сетевых элементов ИТКС можно представить случайным процессом [1], 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. Рассмотрим указанные компоненты случайного процесса:

тренд случайного процесса (рис. 1, *a*) – некоторая детерминированная компонента, не содержащая периодических составляющих, кроме, тех, периоды которых заведомо больше интервала временного окна наблюдения случайного процесса;

периодическая (циклическая) компонента (рис. 1, *b*) – определяется как совокупность неслучайных гармонических колебаний, периоды которых заведомо меньше, чем интервал временного окна наблюдения случайного процесса;

случайная компонента (рис. 1, *c*) – центрированный случайный процесс.

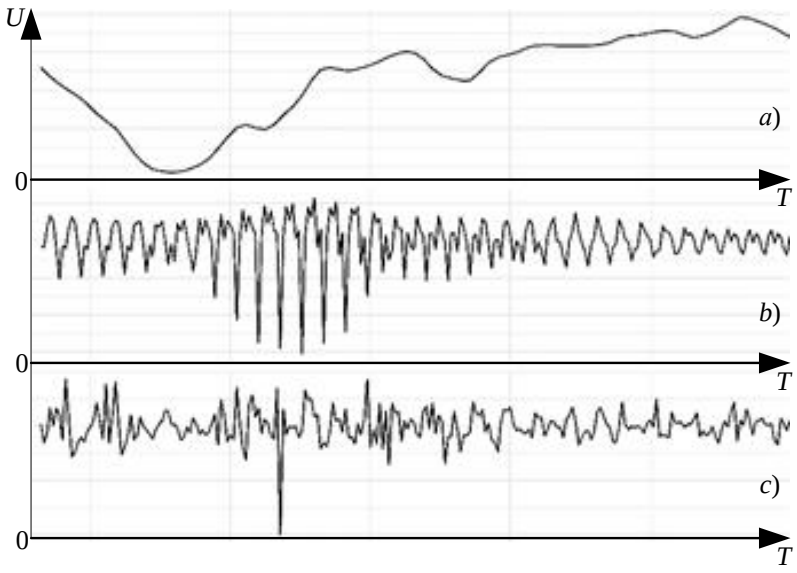


Рис. 1. Основные разновидности случайных процессов, представляемые временными рядами

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 [2]) 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 интенсивность отказов элементной компонентной базы (ЭКБ) и состоящих из нее сетевых элементов носит как раз периодический характер. Трендовая компонента в таких рядах, как правило, является монотонной, имеет постоянные либо сравнительно медленно меняющиеся значения параметров, связанные с деградационными процессами в ЭКБ (рис. 1, *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.

Цель статьи: выработка подхода к формированию методики прогнозирования (превентивной идентификации) аномальной ситуации во временном ряду метрик сетевых элементов на основе анализа научно-методического аппарата обработки временных рядов серверами мониторинга информационно-телекоммуникационных сетей общего пользования.

1. Анализ научно-методического аппарата решения задач прогноза временных рядов

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

Метод Винтерса или обобщенный метод экспоненциального сглаживания [3], 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 тоже 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*) [4]. АРПСС уходит от экспоненциального сглаживания, однако, при этом учет периодической компоненты также 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 [5] 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*) [6]. 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: $X \subseteq R^d$) представляют в виде множества точек в заданном топологическом пространстве (например, пространстве метрик сетевых элементов ИТКС), к которому применимы процедуры *TDA*. А поскольку в *UEBA* исходные данные в основном представлены временными рядами, то временной ряд преобразуется без потери информации в облако точек, рис. 2, где каждому элементу в облаке данных ставится в соответствие точка в соответствующем облаке.

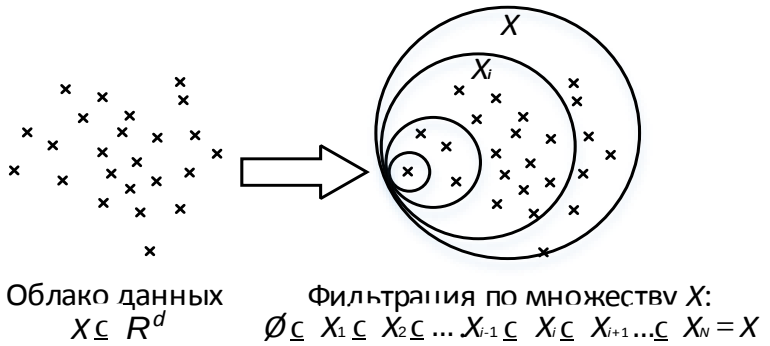


Рис. 2. Общая схема *TDA*

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 [7] или алгоритма ложных соседей [8]). 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 топологических 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 [9], метрик Вассерштейна [10], Чебышева [6] и других методов, выявляют отклонения текущего (наблюдаемого) от базового профиля поведения.

В последнее время для прогнозирования временных рядов также широко используются ***нейросетевые алгоритмы*** [11-14]. 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. 3 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.

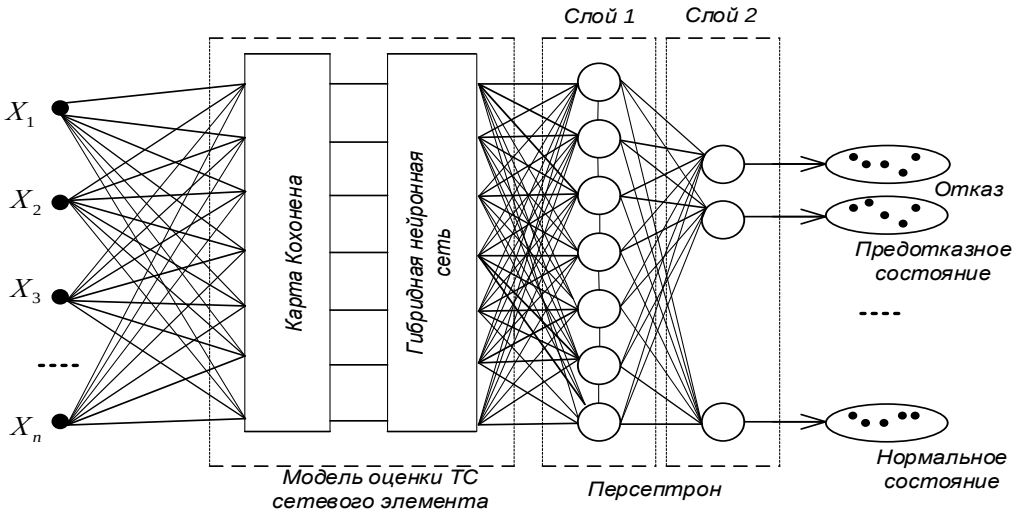


Рис. 3. Модель прогнозирования технического состояния сетевого элемента

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. Исходя из задач прогнозирования ТС сетевого элемента в [11-13] 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 ТС сетевого элемента [12, 13].

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 [14] позволяет повысить контрастность классов ТС и получить более гарантированную оценку, рис. 4.

Достаточно активно при исследовании прогнозирования временных рядов на сегодня используется подход ***кластерного анализа*** [15, 16], 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) [17]. 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 [18], 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.

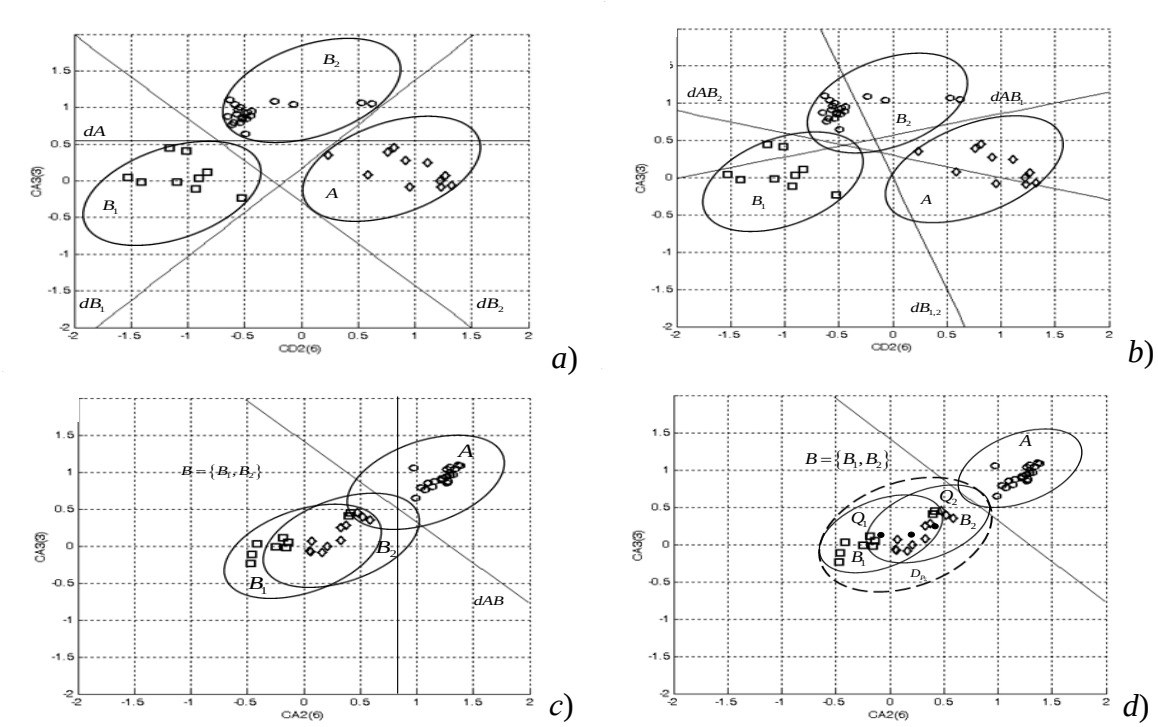


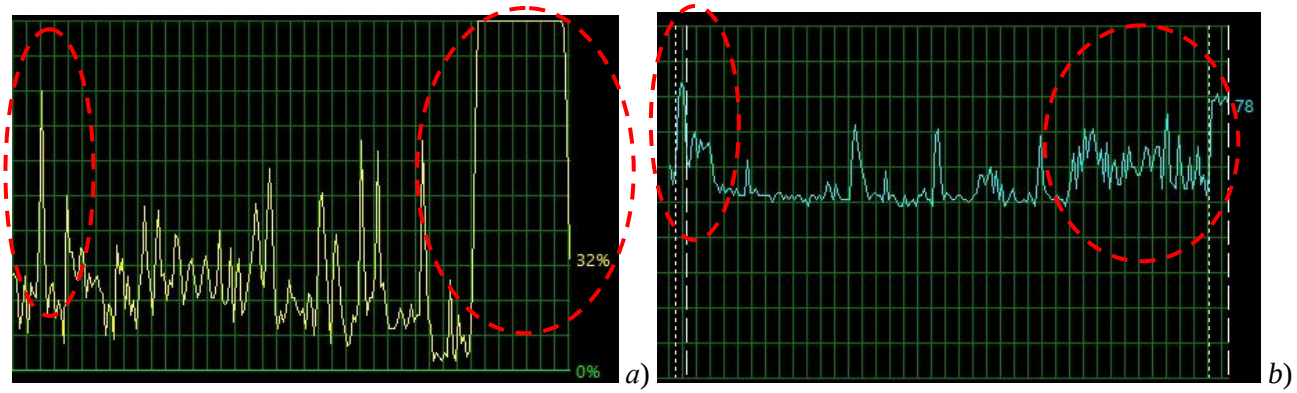
Рис. 4. Применение ДВП для разделение классов ТС в виде областей работоспособности [14]: *a*) неперекрывающихся; *d*) частично перекрывающихся, *c*) перекрывающихся; *d*) объединенных (на рисунке обозначены: A – работоспособное, B_1 – неработоспособное, B_2 – предотказное ТС)

В ходе последующего кластерного анализа осуществляется выделение кластеров, элементами которых являются временные ряды одной и той же метрики, 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 [19].

В системах поведенческой аналитики [20] 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: $H_1(O_1) = \langle h_{11}, h_{12}, \dots, h_{1m}, \rangle$; $H_2(O_2) = \langle h_{21}, h_{22}, \dots, h_{2m}, \rangle$; …; $H_n(O_n) = \langle h_{n1}, h_{n2}, \dots, h_{nm}, \rangle$, и которые определяют реализацию дальнейших действий. В качестве характеристик могут рассматриваться как внешние, так и внутренние признаки (рис. 5), позволяющие проводить анализ текущего состояния объекта мониторинга, и по аномальным отклонениям одной метрики идентифицировать изменения в поведении временного ряда другого параметра. 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.



a) *b*)

Рис. 5. График изменения загрузки процессора (*a*) и его температурного режима (*b*)

Тогда на основе поведенческого подхода [20] задача определения технического состояния (ТС) сетевого элемента ставится следующим образом. Пусть C – множество классов состояний, характеризуемое в соответствие с [2] как «исправное», «работоспособное», «предотказное», «предельное» и т. д., или в соответствии с [21] – 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 $Z^k = \{z_1, z_2, \dots, z_m\} \in Z$. 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 [22]. 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 [20].

2. 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 [11]. В [23] 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 экспертных 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 ИНС. Здесь процедура оценивания ТС основана на методах экспертных оценок, статистических методах распознавания, метрических методах, методах статистических решений (Неймана-Пирсона, минимакса), а также ИНС [11, 23];

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), см. табл. 1, поступающего от объекта мониторинга (при степени неоднородности от 0,7 до 1), наиболее применим метод дискретных вейвлет-преобразований (ДВП), а также метод последовательного анализа Вальда [11, 23].

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);

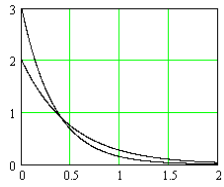
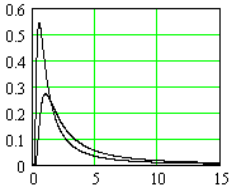
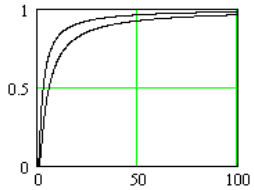
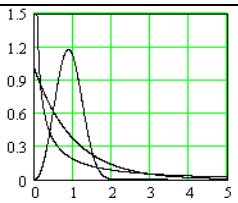
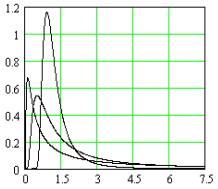
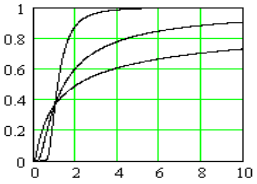
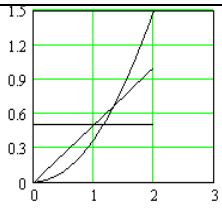
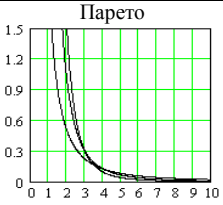
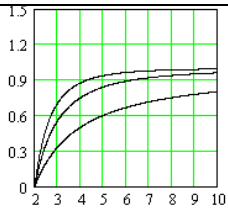
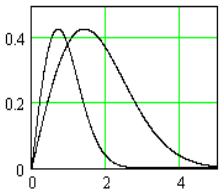
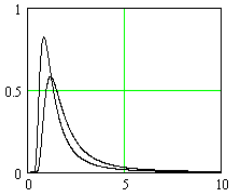
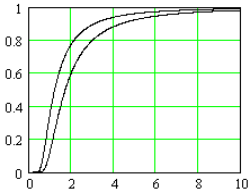
возможности регуляризации временного ряда по небольшому числу параметров.

наличия теоретически обоснованного алгоритма оптимизации.

3. Символьное представление временных рядов

Рассматривая поведенческий подход к мониторингу ИТКС, необходимо отметить, что независимо от отечественной или международной классификации состояний технических устройств [2, 21], в итоге, интерпретация таких состояний 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 состояний и о направлении динамики процесса – от «нормы» к «аварии», от «аварии» к «норме».

Таблица 1 – Примеры законов распределения потока измерительной информации, характеризующих аварийную ситуацию [24]

№ п/п	Законы распределения	Исходный закон распределения $f(x)$	Плотность распределения интервалов времени $g(\tau)$	Функция распределения $G(\tau)$
1.	Экспоненциальный	 $f(x)=\lambda e^{-\lambda x}$, $\lambda = 2, 3$	 $g(\tau)=\frac{\lambda L_0}{\tau^2}e^{-\frac{\lambda L_0}{\tau}}$	 $G(\tau)=e^{-\frac{\lambda L_0}{\tau}}$
2.	Вейбулла	 $f(x)=C\alpha x^{\alpha-1}e^{-cx^2}$ $C=2;\ \alpha=1,2,3$	 $g(\tau)=C\alpha\frac{L_0^{\alpha}}{\tau^{\alpha+1}}e^{-\frac{CL_0^{\alpha}}{\tau^{\alpha}}}$	 $G(\tau)=e^{-\frac{CL_0^{\alpha}}{\tau^{\alpha}}}$
3.	Исходный	 $f(x)=ax^{a-1}$, $a=1, 2, 3$	Парето  $g(\tau)=\frac{ab^a}{\tau^{a+1}}$, $a=2, 4$	 $G(\tau)=1-\left(\frac{b}{\tau}\right)^a$, $a=2, 4$
4.	Рэлея	 $f(x)=\frac{x}{\sigma^2}e^{-\frac{x^2}{2\sigma^2}}$, $\sigma=1,2$	 $g(\tau)=\frac{d}{\tau^3}e^{-\frac{d}{2\tau^2}}$, $d=1,2$	 $G(\tau)=e^{-\frac{d}{2\tau^2}}$

Динамика переходных процессов от «нормы» (*N*) к «аварии» (*F*) [21] 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 тоже 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. 1 *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»), но даже он не приводит к надежной идентификации направления динамики процесса.

Нужен поиск новых подходов к решению такого класса задач.

Рассмотрим временной ряд с использованием символьного представления, описанного в [25] и применяемого в разделе символической динамики из теории динамических систем, 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 технического состояния (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 (метрик).

Данная оценка была заимствована теорией символической динамики из биоинформатики, где активно используется для оценки сложности нуклеотидных геномных последовательностей [26], например, очень длинных последовательностей ДНК [27], рис. 6.

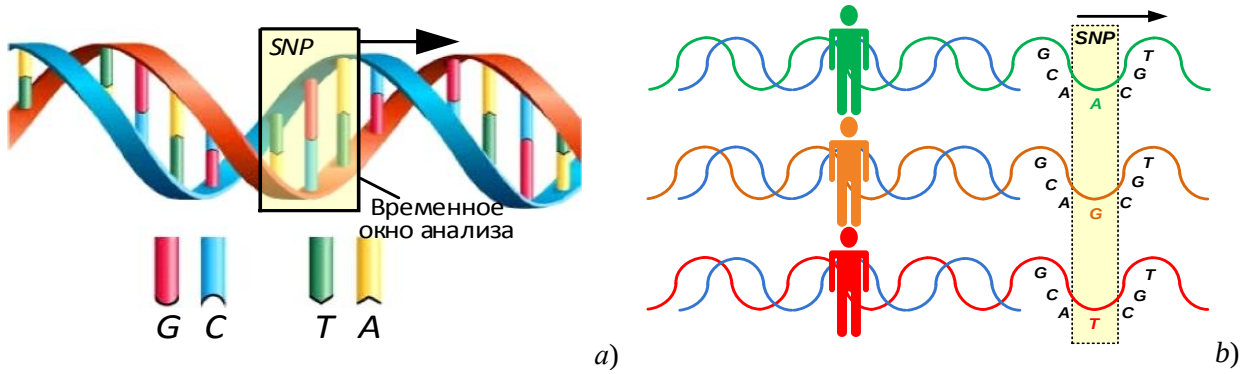


Рис. 6. Процесс анализа сложных нуклеотидных геномных последовательностей методом символической динамики

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 оценена с помощью топологической энтропии или метрической энтропии по Колмогорову [28].

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 ТС).

Для решения задачи на первом этапе осуществляем символьное кодирование временного ряда по возможным значениям параметров (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 тоже 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 различных интервалах времени t_i, что видно из рис. 7.

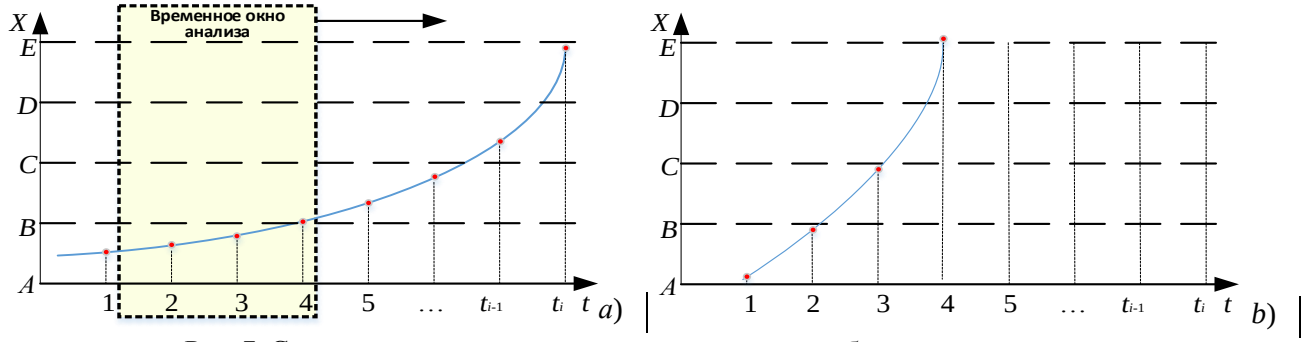


Рис. 7. Символьное представление временного ряда наблюдаемого параметра
a) с медленным и *b*) лавинообразным нарастанием аварийной ситуации (отказа элемента)

Для универсализации временных рядов в [25] 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 $y_{min} = \min\limits_{i=1,n} f_i$, $y_{max} = \max\limits_{i=1,n} f_i$, 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 правильнее рассматривать диапазон $[y_i, y_{i+1}) = \{y \,|\, y_i \le y < y_{i+1}, i = 1,\ldots, m-1\}$. В данном случае 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 [18] с применением бикритериального метода построения гистограмм [29], которая уже была решена в [29]. Число разбиений k диапазона наблюдения параметра, полученных данным методом и определяет мощность алфавита описания.

Например, на рис. 7 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. 7 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 (в соответствии с [2] соответствует исправному ТС 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. 7 *a*) – {*AAABBBCD*…}; для рис. 7 *b*) – {*AABE*…}. Если наблюдаемый процесс описывается резким увеличением значений параметра (наблюдаемой величины), равно как и резким спадом за один временной интервал относительно нормального 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. 7 *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 слове-строке временного ряда. 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. 7 а) 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 [30], 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 слове-строке временного ряда может лечь в основу метода прогнозирования наступления аварии или отказа.

Для решения задачи масштабирования в [28] 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 [30]. Число разбиений при оценке функциональной надежности сетевых элементов как правило соответствует видам их ТС [2, 21].

Как отмечалось ранее, в соответствие с [2] различают следующие виды технического состояния: исправное, неисправное, работоспособное, неработоспособное, предельное, опасное и предотказное состояние. В тоже время, с точки зрения функциональной надежности нас в большей степени интересует переход из работоспособного в неработоспособное («Авария» или «Отказ») состояние через промежуточное – предотказное ТС. Учитывая это, разбиение, соответствующее предотказному техническому состоянию может уточняться для каждого сетевого элемента или его измеряемого параметра. 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 [28] осуществлен переход от оценки абсолютной сложности строки по Колмогорову (от длины сжатой строки) к ее относительной оценке через коэффициент сжатия [15, 16].

4. 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 [28] 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. 8.

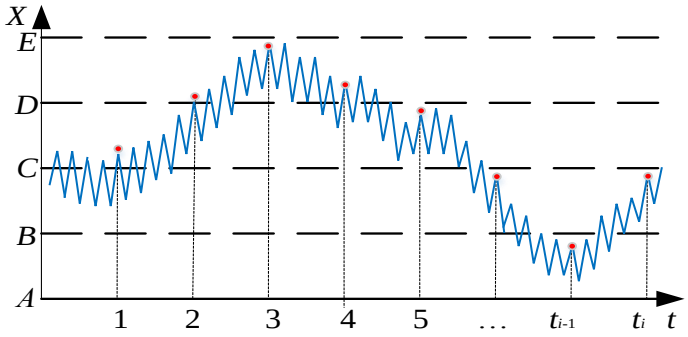


Рис. 8. Символьное описание временного ряда изменения значения параметра

Для кодирования *по тенденциям* представленного на рис. 8 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 + 0 0 – – – +}, 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 [2].

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 (аварии). 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 ОК (для рассматриваемого примера рис. 7 и 8 – разбиение «*E*»). Так, при символьном кодировании значений временного ряда на рис. 7 *a*) факт перехода из режима нормального функционирования (символ разбиения – «*A*») к предотказному состоянию (символ разбиения «*D*») интерпретируется слогом «*BCD*» в слове-строке {*AAABBBCD*…}, а на рис. 7 *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.

5. 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 [18].

При этом оценку энтропии кодовых слов описывающего временной ряд наблюдаемого параметра осуществляют в следующем порядке [18]. 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 возрастает 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 [31], функцию $C(m)$ называют оценкой энтропии сдвигов.

6. Алгоритм превентивной идентификации аномальной ситуации на временном ряду метрик

Исходя из рассмотренных методов анализа временных рядов предложен алгоритм превентивной идентификации аномальной ситуации на временном ряду метрик. Блок-схема алгоритма состоит из четырех этапов: предварительного этапа, этапа кодирования временных рядов, этапа идентификации состояния сетевого элемента и завершающего этапа, рис. 9.

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 [30]; 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); классах (видах) технического состояния сетевого элемента; используемых протоколах сбора измерительной информации и др.

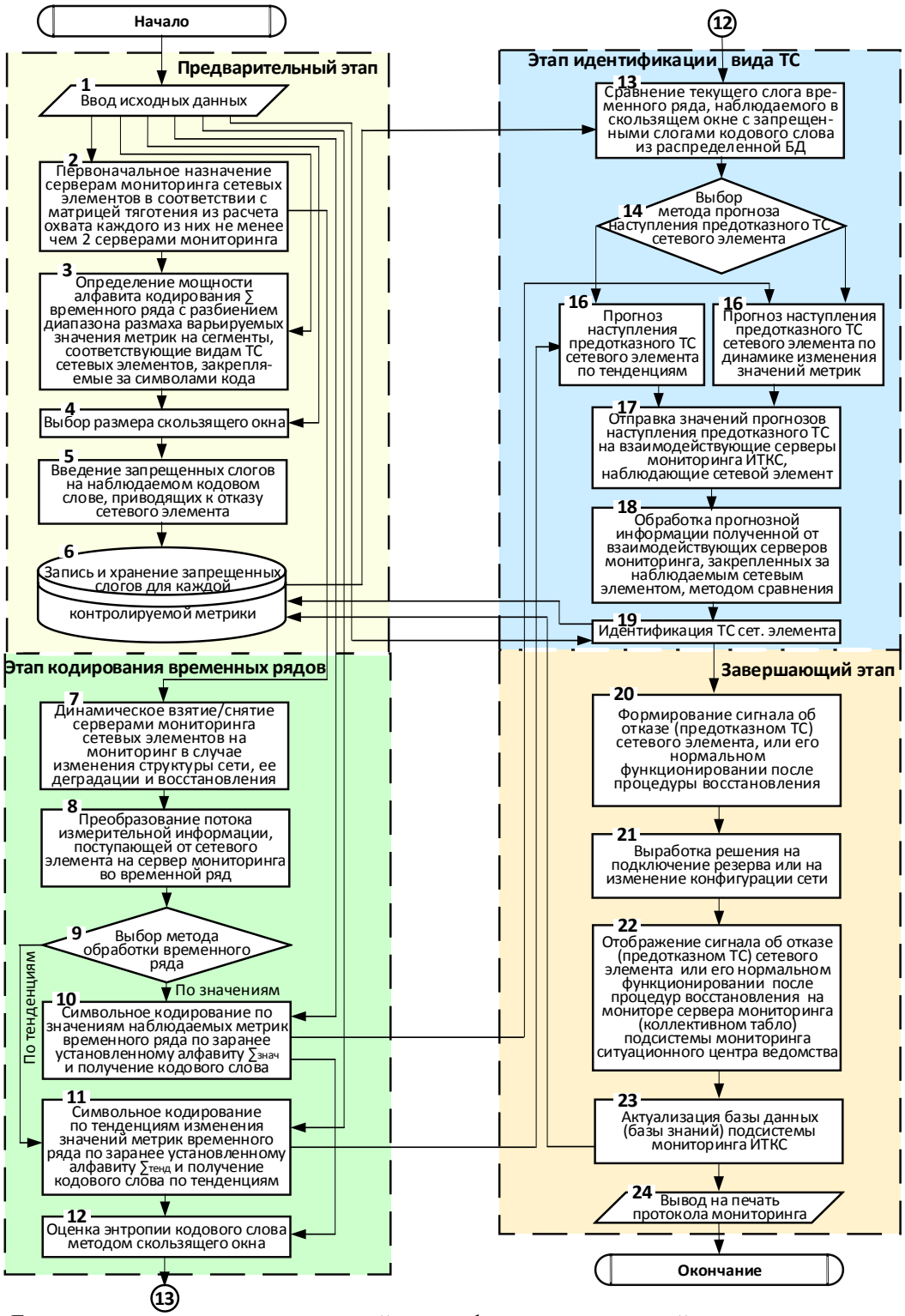


Рис. 9. Блок-схема алгоритма превентивной идентификации аномальной ситуации на временном ряду

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) ТС сетевых элементов, закрепляемые за символами кода. Соотнесение классов (видов) ТС [2] с символами выбранного алфавита Σ кодирования временного ряда.

Выбор размера скользящего окна (по методике Сметанина Ю.Г., Ульянова М.В. [29] 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.

Запись и хранение запрещенных слогов для каждой контролируемой метрики каждого сетевого элемента в распределенной базе данных (БД) (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 временной ряд, 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 $\Sigma_{знач}$ и получение кодовых слов-строк по значениям.

Символьное кодирование по тенденциям изменения значений метрик временного ряда символами ранее установленного алфавита $\Sigma_{тенд.}$ 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 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 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 данный шаг выполняется параллельно с предыдущим.

Отображение сигнала об отказе (предотказном техническом состоянии) 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 техническом состоянии сетевых элементов ИТКС, обновление структуры сети в связи с последними изменениями (отказом, резервированием, восстановлением), динамическое перезакрепление серверов мониторинга за сетевыми элементами в связи с динамикой изменения состояния ИТКС (изменение матрицы тяготения серверов мониторинга и сетевых элементов), уточнение исходных данных алгоритма, обновление и репликация распределенной базы данных ИТКС.

Вывод на печать протоколов мониторинга.

Заключение

Таким образом, 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 рядов, 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 технического состояния 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.

Литература

1. Игнатов Н.А. Прогнозирование временных рядов с регулярными циклическими компонентами с помощью модели периодически коррелированных случайных процессов // Научные труды: Институт народнохозяйственного прогнозирования РАН, 2011.

2. ГОСТ 27.002-2015 Надежность в технике. Термины и определения. Москва: Стандартинформ. 2016. 23 с.

3. Батурин А. Прогноз по методу экспоненциального сглаживания с трендом и сезонностью Хольта-Винтерса [электронный ресурс] URL:https://4analytics.ru/prognozirovanie (Дата обращения 03.03.2021).

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

5. 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.

6. Нашивочников Н.В., Пустарнаков В.Ф. Топологические методы анализа в системах поведенческой аналитики // Вопросы кибербезопасности. 2021. № 2 (42). С. 26-36.

7. Макаренко Н.Г. Эмбедология и нейропрогноз. Часть 1. – М. МИФИ. 2003. 188 с.

8. 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. https//doi:org/10.1155/2015/932750.

9. Пичкалев А.В. Применение кривой желательности Харрингтона для сравнительного анализа автоматизированных систем контроля // Вестник НГТУ. – Красноярск: КГТУ. 1997. № 1. С. 128-132.

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

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

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

13. 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.

14. 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.

15. 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.

16. 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.

17. 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 (Дата обращения 30.04.2021).

18. 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.

19. 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).

20. 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.

21. Рекомендация [Рек. М.3703] – М.3703: Common management services – Alarm management – Protocol neutral requirements and analysis [Электронный ресурс]. URL: https://www.itu.int/rec/T-REC - M.3703 – 201006-I. (Дата обращения 14.05.2021).

22. Нашивочников Н.В., Большков 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.

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

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

25. 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.

26. 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.

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

28. 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.

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

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

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

References

1. Ignatov H. A. Forecasting of time series with regular cyclic components using a model of periodically correlated random processes. Scientific works: Institute of National Economic Forecasting of the Russian Academy of Sciences, 2011 (in Russian).

2. GOST 27.002-2015 Reliability in technology. Terms and definitions. Moscow: Standartinform. 2016. 23 p. (in Russian).

3. Baturin A. Forecast by the exponential smoothing method with the Holt-Winters trend and seasonality [electronic resource] URL: https: / / 4analytics. ru / forecasting (Accessed 03.03.2021) (in Russian).

4. Yakovleva A.V. Econometrics. Abstract of lectures. Moscow: EKSMO, 2008. - 244 p. (in Russian).

5. Kashkin V. B., Rubleva T. V. Application of singular spectral analysis for the identification of weakly expressed trends. Izvestiya Tomsk Polytechnic University. 2007. Vol. 311. No. 5. Pp. 116-119 (in Russian).

6. Nashivochnikov N. V., Pustarnakov V. F. Topological methods of analysis in behavioral analytics systems. Cybersecurity issues. 2021. No. 2 (42). Pp. 26-36 (in Russian).

7. Makarenko N. G. Embedology and neuroprognosis. Part 1. M. MEPhI. 2003. 188 p. (in Russian).

8. Krakovskaya A., Mezeeva K., Budakova N. Using False nearest neighbors to select variables and embed parameters to restore the state. Journal of Complex Systems, 2015. pp. 1-12. https// doi: org/10.1155/2015/932750.

9. Pichkalev A.V. Application of the Harrington desirability curve for comparative analysis of automated control systems. Bulletin of the NSTU. Krasnoyarsk: KSTU. 1997. No. 1. Pp. 128-132 (in Russian).

10. Arzhovsky M., Chintala S., Bottu L. Wasserstein Generative adversarial networks // Proceedings of the 34th International Conference on Machine Learning, PMLR. 2017. Pp. 214-223.

11. Vinogradenko A.M. Methodology of intellectual control of the technical condition of the automated communication system for special purposes. Monograph. - St. Petersburg: High-tech technologies, 2020. - 180 p. (in Russian).

12. Kotenko I., Saenko I., Ageev S. Application of fuzzy computing methods for operational monitoring of network elements of a new generation. In: Achievements in the field of intelligent systems and computer technology. 2018. Volume 874. Springer, Cham. Pp. 331-340.

13. Kotenko I., Saenko I., Ageev S. Monitoring of the state of elements of multiservice communication networks based on fuzzy logical inference. In the book: Materials of the Sixth International Conference on Communications. Computing, Networks and Technologies (INNOV-2017). 2017. Pp. 26-32.

14. Kotenko I. V., Budko P. A., Vinogradenko A.M., Saenko I. B. An approach to the intellectual assessment of the state of complex autonomous objects based on wavelet analysis / / 18th International Conference on Methodologies, Tools and Methods of Intelligent Software (SOMET ' 2019) - Kuching, Sarawak, Malaysia, September 23-25, 2019, pp. 25-38.

15. Grabust P. Methods of estimating the similarity of time series. Scientific works Interd. Conf. "The theory of probability, stochastic processes, mathematical statistics and applications", Minsk, BSU, 15-19 September 2008, Minsk: Belarusian state University, 2008. Pp. 23-24 (in Russian).

16. Ulyanov, V., Smets, Y. G. On one approach to the construction of a clustered space time series: Kolmogorov and harmonic complexity. Materials of the International scientific-practical conference "Information control systems and technologies" (ICST 2013). Odessa, 2013. Pp. 30-36 (in Russian).

17. 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 Electronics and Electrical Engineering, University College London, UK. 2017 (Accessed 30.04.2021) (in Russian).

18. Smetanin Yu. G., Ulyanov M. V. The measure of symbolic diversity: an approach of combinatorics of words to the definition of generalized characteristics of time series. Business Informatics. 2014. No. 3 (29). Pp. 40-48 (in Russian).

19. Behavioral Analysis Systems Market Overview-Behavioral Analytics of Users and Organizations (UBA / UEBA) November 23, 2017. URL: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba (Accessed 04.07.2021) (in Russian).

20. Sukhoparov M.E., Lebedev I. S. Models of analysis of the functional state of elements of devices of networks and telecommunications "Industry 4.0": monograph. St. Petersburg: Polytech-Press, 2020. - 121 p. (in Russian).

21. Recommendation [Rec. M. 3703] - M. 3703: General management services-Alarm management - Requirements and analysis of protocol neutrality [Electronic resource]. URL: https://www.itu.int/rec/T-REC -M. 3703-201006-I. (Accessed 14.05.2021) (in Russian).

22. Nashivochnikov N.V., Bolshkov A. A., Nikolashin Yu. A., Lukashin A. A. Problematic issues of the use of analytical security tools for cyber-physical systems of fuel and energy complex enterprises. Issues of cybersecurity. 2019. No. 5 (33). Pp. 26-33 (in Russian).

23. Podinovsky V.V. Ideas and methods of the theory of the importance of criteria in multi-criteria decision-making problems. Moscow: Nauka, 2019. 103 p. (in Russian).

24. Budko P.A. Resource management of information and telecommunications systems. Optimization methods: Monograph. - St. Petersburg: VAS, 2012 – 512 p. (in Russian).

25. Smetanin Yu. G., Ulyanov M. V. Entropic characteristics of diversity in the symbolic representation of time series. Modern information technologies and IT education. 2014. No. 10. pp. 426-436 (in Russian).

26. Orlov Yu. l. Computer implementation estimates the complexity of the texts. Proceedings of the Russian NTK "Discrete analysis and operations research" (DAOR), Novosibirsk, Institute of mathematics, 28 June – 2 July, 2004 Novosibirsk: Izd-vo Inst mathematics SB RAS, 2004. P. 225 (in Russian).

27. Mathematical methods for the analysis of DNA sequences. M.: Mir, 1999. 349 p. (in Russian).

28. Ulyanov M.V., Smetanin Yu.G. 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).

29. Petrushin V.N., Ulyanov M.V. Bicriteria method of constructing histograms. Information technologies and computing systems. 2012. No. 4. Pp. 22-31 (in Russian).

30. Abramov O.V., Rosenbaum A.N. Management of the operation of responsible purpose systems. Vladivostok: Dalnauka, 2000 (in Russian).

31. Lind D., Markus B. Introduction to symbolic dynamics and coding. Cambridge, UK: Cambridge University Press, 1995. 495 p.

Статья поступила 24 апреля 2021 г.

Информация об авторе

Аллакин Владимир Васильевич – Соискатель ученой степени кандидата технических наук. Независимый специалист. E-mail: vladimir@duduh.ru. Адрес: 188660, Ленинградская обл., Всеволожский район, пос. Бугры, ул. Школьная, дом 11, корп. 1, кв. 510.

Analysis of methods for estimating time series by the monitoring server of a public information and telecommunications network

V.V. Allakin

Annotation. Task statement: *based on the analysis of the scientific and methodological apparatus for evaluating the time series of the observed metrics, to develop an approach to the formation of a methodology for predicting (preventive identification) of abnormal situations based on the results of monitoring the functional state of network elements of public information and telecommunications networks.* ***The purpose of the work:*** *to develop an algorithm for identifying an abnormal situation by the monitoring server based on the observed time series of metrics of network elements.* ***Methods used:*** *methods of analysis theory, forecast theory, reliability theory, diagnostic theory, classification theory, cluster analysis methods, topological methods of time series analysis, behavioral analytics methods, symbolic representation of time series.* ***Novelty:*** *preventive identification of the abnormal state of a network element by identifying "forbidden" code combinations during the observation of time series processed by symbolic dynamics methods borrowed from bioinformatics, previously used in the analysis of complex nucleotide genomic sequences, as well as the introduction of 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 to prevent the failure of the network element from being missed or the occurrence of a network accident on the network.* ***Results:*** *the analysis of the scientific and methodological apparatus for solving time series forecasting problems was carried out, as a result, in order to achieve the set research goal, a method of symbolic representation of time series was chosen, on the basis of which the entropy of code words describing the time series of the observed parameter of a functioning network element was estimated, and an algorithm for identifying an anomalous situation on a time series of metrics was developed, consisting of four stages: the preliminary stage, the stage of encoding time series, the stage of identification of the type of technical condition of the network element and the final stage.* ***Practical significance:*** *the analysis of time series estimation methods presented in the paper allowed us to develop an approach to constructing an algorithm for the functioning of a monitoring server to identify anomalies in the operation of the observed peripheral equipment of a public information and telecommunications network.*

Keywords: *monitoring server, time series, prediction of an abnormal situation, preventive identification of the type of technical condition, special monitoring mode.*

Information about Authors

Vladimir Vasilyevich Allakin – Doctoral Student. Independent Expert. E-mail: vladimir@duduh.ru. Address: 188660, Russia, Leningrad region, Vsevolozhsky district, vil. Buhry, Shkolnaya str., 11, build. 1, sq. 510.

Для цитирования: Аллакин В.В. Анализ методов оценки временных рядов сервером мониторинга информационно-телекоммуникационной сети общего пользования // Техника средств связи. 2021. № 2 (154). С. 60-80.

For citation: Allakin V.V. Analysis of methods for estimating time series by the monitoring server of a public information and telecommunications network. Means of Communication Equipment. 2021. No. 2 (154). Pp. 60-80 (in Russian).

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ

УДК 621.396

Об основах методологии повышения качества программных систем

Фортинский А.Г., Билятдинов К.З. Спивак А.И.

Аннотация. *В работе дано соответствие понимания программной системы, под которой предлагается понимать систему, состоящую из программного обеспечения и компьютерного оборудования для его выполнения. Актуальность темы происходит из-за высокой степени автоматизации процессов управления в последнее время и увеличения, как объемов обрабатываемой информации, так и количества источников информации. Вследствие этого возникает необходимость эффективного развития и совершенствования математического и программного обеспечения вычислительных машин, комплексов и компьютерных сетей. Оценку качества программных продуктов предлагается проводить в несколько этапов. На первом этапе проводится выбор показателей. На втором этапе осуществляется расчет их действительных значений. На третьем реализуется сравнение их с базовыми показателями (требованиями). На четвертом этапе (при необходимости) производится определение (уточнение) этих базовых показателей (требований), учитывая специфику и условия функционирования системы управления. На основе предложенных этапов оценки программной системы в статье рассмотрены основные актуальные научно-методологические аспекты применения апробированных методологических решений в сфере оценки качества в интересах повышения (обеспечения) качества программных систем в процессе эксплуатации. Сформулировано определение методологии и возможные направления рационального использования. В методологии предлагается повышение качества программных систем обеспечивать за счет принятия своевременных обоснованных управленческих решений по результатам оценки качества программных систем в процессе эксплуатации. В статье отмечена практическая направленность предлагаемой методологии повышения качества программных систем, вследствие развития и использования современных технологий, что обеспечивает предпосылки для повышения ее универсальности при применении большого количества разнообразных программных систем в составе взаимодействующих систем управления различного назначения.*

Ключевые слова: *оценка качества, риск системы, программная система, управленческое решение, ошибки первого и второго рода*

Введение

Сегодня эффективность современной системы управления в значительность степени зависит от качества программных систем, эксплуатируемых в ее составе.

В данной статье для единообразного понимания применяемой терминологии, целесообразно отметить, что в соответствии с ГОСТ Р 51904-2002 «Программное обеспечение встроенных систем. Общие требования к разработке и документированию» программная система – это система, состоящая из программного обеспечения и компьютерного оборудования для его выполнения.

Актуальность темы

В конце XX – начале XXI века произошло значительное увеличение влияния качества программных систем на функционирование органов государственного и военного управления. Это произошло вследствие высокой степени автоматизации процессов управления и увеличения, как объемов обрабатываемой информации, так и количества источников информации. Отсюда возникает необходимость эффективного развития и совершенствования математического и программного обеспечения вычислительных машин, комплексов и компьютерных сетей, применяемых в составе автоматизированных систем управления органов государственного и военного управления.

Вышеприведенные обстоятельства обуславливают актуальность разработки новых универсальных путей повышения качества программных систем в процессе эксплуатации без существенных затрат дополнительных ресурсов и времени. Для этого целесообразно решить задачу разработки и внедрения методологии повышения качества программных систем.

Основы предлагаемой методологии могут состоять в том, что в современных условиях одним из рациональных направлений повышения качества программных систем является принятие своевременных и обоснованных управленческих решений по повышению качества программных систем непосредственно в процессе эксплуатации. При этом на практике в большинстве случаев управленческие решения принимаются лицом, принимающим решения (ЛПР), на основе результатов оценки качества программных систем в процессе их эксплуатации по предназначению. Соответственно, уменьшение затрат ресурсов и времени на оценку качества будет являться определяющим фактором для достижения требуемого положительного эффекта в исследуемой предметной области.

Очевидно, что объективная оценка качества программных систем в основном возможна на этапе эксплуатации. На этом этапе жизненного цикла особенно важно провести оценку качества программных систем в минимальные сроки, что позволит ЛПР, принять своевременные и обоснованные управленческие решения.

Таким образом существует объективная потребность в разработке методологии повышения качества программных систем, в том числе позволяющей провести оценку качества в период эксплуатации за минимальное время при заданных минимальных ресурсах. Все более широкое применение программных систем с целью повышения эффективности управления усиливает актуальность создания и использования данной методологии как важнейшей части математического и программного обеспечения оценки качества [1, 2].

Основные этапы оценки качества программных продуктов

Оценка качества программных продуктов будет включать в себя выбор показателей, расчет их действительных значений, сравнение их с базовыми показателями (требованиями) в сфере обеспечения эффективности управления, а при необходимости и определение (уточнение) этих базовых показателей (требований), учитывая специфику и условия функционирования системы управления.

С учетом важности и сложности систем управления оценку качества программных систем в их составе целесообразно проводить на основе оценки изменения количественных значений выбранных показателей оценки эффективности системы управления после ввода в эксплуатацию оцениваемых программных систем, в процессе их эксплуатации и (или) после модернизации программных систем. Однако, в процессе сопровождения программных систем на этапе эксплуатации ЛПР необходимо получать и использовать большое количество информации об их качестве, поступающей из различных источников. Так как, развитие современных информационных технологий привело к тому, что большинство программных систем, входящих в системы управления, имеют аналоги, в том числе по условиям эксплуатации. Основная часть такой информации размещена на внешних информационных ресурсах, включая информационно-телекоммуникационную сеть «Интернет» [1, 2].

Вышеприведенные обстоятельства не позволяют в полной мере использовать апробированные методы оценки качества и теории надежности [3-8], что усложняет оценку качества программных систем при сопровождении оцениваемых систем в процессе их эксплуатации. Исходя из этого, методология повышения качества программных систем в процессе эксплуатации должна представлять собой учение об организации деятельности в области методологического, математического и программного обеспечения оценки качества в интересах принятия ЛПР своевременных и обоснованных управленческих решений.

Отсюда можно сделать вывод, что основой создания и внедрения методологии будет также являться необходимость выполнения совокупности условий по рациональному

использованию больших объемов статистической и экспертной информации, полученной из множества различных источников.

В свою очередь увеличение объемов информации и количества их источников приведет к существенному увеличению расхода времени и ресурсов. Дополнительно потребуется повышение квалификации ЛПР и персонала, проводящего оценку качества и обеспечивающего принятие управленческих решений.

Поэтому следующим теоретическим базисом для создания методологии повышения эффективности программных систем будет выступать требование по обеспечению возможности применения элементов методологии по трем направлениям повышения (обеспечения) качества программных систем:

1) повышение эффективности управления, эксплуатации и технического обеспечения программных систем в составе системы управления;

2) повышение качества НИОКР по созданию и модернизации программных систем;

3) повышение качества подготовки персонала в сфере эксплуатации и технического обеспечения программных систем.

В качестве комментария важно отметить, что мировой опыт, накопленный специалистами по управлению качеством, свидетельствует о том, что «…устранение … ошибки (допущенной на первом этапе жизненного цикла системы) в процессе выполнения работ на втором этапе в среднем обойдется в 10 раз дороже» [9].

В перспективе результаты применения методологии можно будет эффективно использовать, начиная с подготовки технических заданий на выполнения НИОКР. Цель применения данных результатов в НИОКР будет заключаться, в первую очередь, в заблаговременном устранении возможных ошибок, ухудшающих качество программных систем, и за счет этого будут созданы условия для достижения требуемого уровня качества на начальных этапах жизненного цикла систем, планируемых для эксплуатации в составе систем управления. В этом случае закладывается научно-методологическая основа снижения риска системы управления. Риском системы управления будем считать вероятность принятия неправильного и (или) несвоевременного решения.

При этом в современной науке отсутствует однозначное и обоснованное понимание риска системы. Что, в частности, подтверждается следующим утверждением Н.Д. Ильенковой: «….следует отметить, что методология исследования риска и рекомендации относительно возможности ее практического использования пока еще в полной мере не сформировались. До сих пор не устоялось однозначное понимание риска» [9]. Поэтому актуальность и практическая направленность теоретического базиса рассматриваемой методологии дополнительно должна состоять в раскрытии термина «риск системы» в отношении последствий от неправильных решений.

В этом случае риск системы управления вследствие принятия неправильного и несвоевременного решения по результатам оценки качества – это вероятность возникновения любого повышенного расхода ресурсов и времени по сравнению с прогнозируемым вариантом и (или) вероятность потери устойчивости функционирования системы управления, а также невыполнения задач по предназначению [1, 2].

При оценке качества и, соответственно, при принятии управленческих решений по результатам этой оценки могут быть ошибки первого и второго рода.

Ошибка первого рода – программная система, которая отвечает требованиям по качеству, может быть ошибочно признана не отвечающим этим требованиям или эффективная система может быть признана неэффективной.

Ошибка второго рода – программная система, которая не отвечает требованиям по качеству, может быть ошибочно признана отвечающим эти требованиям или неэффективная система может быть признана эффективной.

Понятие риска системы управления напрямую связано с вероятностью принятия неправильного решения, которое влечет ошибки первого или второго рода.

С учетом того, что своевременное решение – это важнейший элемент обеспечения эффективности систем управления, то, следовательно, уменьшение времени оценки будет выступать дополнительным важнейшим фактором снижения вероятности ошибок первого рода, а значит, повышения эффективности управления. В то же время эффективность любой системы будет связана с существенным изменением количественных показателей, характеризующих затраты всех видов ресурсов и затраты времени. Оценка качества обеспечивает некоторый полезный эффект, связанный, в свою очередь, с затратами. Сопоставление полезного эффекта с затратами на его получение позволяет судить об эффективности системы управления, в составе которой эксплуатируются оцениваемые программные системы. Таким образом, прослеживается взаимосвязь между эффективностью системы и направленностью на снижение риска этой системы в процессе эксплуатации [1, 2].

Вывод

В заключении важно отметить, что актуальность и практическая направленность предлагаемой методологии дополнительно основана на том, что при реализации предлагаемых подходов в процессе эксплуатации будут формироваться информационные резервы повышения качества программных систем, подготовки квалифицированных кадров, обеспечения научно-исследовательских и опытно конструкторских работ по совершенствованию и развитию программных систем в составе систем управления с учетом специфики эксплуатации. В перспективе методология повышения качества программных систем станет еще более востребованной вследствие развития и использования современных технологий, которые обеспечивают предпосылки для повышения ее универсальности при применении большого количества разнообразных программных систем в составе взаимодействующих систем управления различного назначения.

Литература

1. Билятдинов К.З., Шлянцев И. Меняйло В.В. О повышении эффективности управления эксплуатацией технических систем // Вестник воздушно-космической обороны. Вып. 4(28). 2020. С. 18-25.

2. Билятдинов К.З., Меняйло В.В. Методология оценки качества систем в сфере устойчивости больших технических объектов // Век качества. 2020. №2. С. 198-214.

3. Деминг Э. Выход из кризиса: Новая парадигма управления людьми, системами и процессами. – М.: Альпина Паблишерз, 2007. – 349 с.

4. Закс Л. Статистическое оценивание. – М.: Статистика, 1976. – 595 с.

5. Месарович М. Теория иерархических многоуровневых систем. – М.: Мир, 1973. – 344 с.

6. Местецкий Л.М. Математические методы распознавания образов: курс лекций [Электронный ресурс] http://www.ccas.ru/frc/papers/mestetskii04course.pdf (дата обращения 19.05.2021).

7. Могилевский В.Д. Методология систем: вербальный подход. – М.: Экономика, 1999. – 251 с.

8. Надежность и эффективность в технике: справочник. Ред. совет: В.С. Авдуевский (пред.) и др. Т. 1. Методология. Организация. Терминология. Под ред. А.И. Рембезы. – М.: Машиностроение, 1986. – 224 с.

9. Математические и инструментальные методы экономического анализа: управление качеством: Сб. науч. тр. Под науч. ред. проф. Б.И. Герасимова. – Тамб. гос. техн. ун-т. Тамбов. 2004. Вып.13. – 240 с.

References

1. Bilyatdinov K.Z., Shlyantsev I. Menyaylo V.V. On improving the efficiency of technical systems operation management. Bulletin of Aerospace Defense, vol. 4 (28), 2020. Pp. 18-25 (in Russian).

2. Bilyatdinov K.Z., Menyaylo V.V. Methodology for assessing the quality of systems in the field of stability of large technical facilities. Quality Century. №2. 2020. Pp. 198-214. (in Russian).

3. Deming E. Getting out of the crisis: A new paradigm for managing people, systems and processes. Moscow. Alpina Pabl., 2007. 349 p. (in Russian).

4. Zax L. Statistical assessment. Moscow. Statistics Pabl., 1976. 595 p. (in Russian).

5. Mesarovich M. Theory of hierarchical multilevel systems. Moscow. World Pabl., 1973. 344 pages.

6. Mestetsky L.M. Mathematical methods of pattern recognition: lecture course. Access mode: http://www.ccas.ru/frc/papers/mestetskii04course.pdf (accessed 19.05.2021) (in Russian).

7. Mogilev V.D. System methodology: verbal approach. Moscow. Economics Publ., 1999. 251 p. (in Russian).

8. Reliability and Efficiency in Technology: Reference. Ed. council: V.S. Avduevsky (before) and others. T. 1. Methodology. Organization. Terminology. Ed. A.I. Rembeza. Moscow. Engineering Publ., 1986. 224 p. (in Russian).

9. Mathematical and instrumental methods of economic analysis: quality management: Sat. scientific. tr. Under scientific. Ed. prof. B.I. Gerasimova. Tamb. State Technician. un-t. Tambov. 2004. Issue 13. 240 p. (in Russian).

Статья поступила 29 мая 2021 г.

Информация об авторах

Фортинский А.Г. – Кандидат технических наук, заместитель генерального директора АО «ЦНИИ ЭИСУ». E-mail: cniieisu@cniieisu.ru. Тел.: +7 (495) 539-22-49. Адрес: Россия, г. Москва, ул. Малая Бронная, д. 2/7, стр.1.

Билятдинов К.З. – Кандидат военных наук, доцент, доцент факультета инфокоммуникационных технологий Национальный исследовательский университет ИТМО. E-mail: od@mail.ifmo.ru. Тел.: +7 (812) 232-97-04. Адрес: Россия, г. Санкт-Петербург, Кронверкский проспект, д.49.

Спивак А.И. – Начальник отдела Центра защиты Государственной тайны НЦУО МО РФ. E-mail: intelteh@inteltech.ru. Тел.: +7(812)313-12-51. Адрес: Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

On the basics of the methodology for improving the quality of software systems

A.G. Fortinsky, K.Z. Bilyatdinov, A.I. Spivak

Annotation. *The paper gives the correspondence of the understanding of the software system, by which it is proposed to understand a system consisting of software and computer equipment for its execution. The relevance of the topic is due to the high degree of automation of management processes in recent years and the increase in both the volume of processed information and the number of information sources. As a result, there is a need for effective development and improvement of mathematical and software software for computers, complexes and computer networks. It is proposed to evaluate the quality of software products in several stages. At the first stage, the selection of indicators is carried out. At the second stage, their actual values are calculated. At the third stage, they are compared with the basic indicators (requirements). At the fourth stage (if necessary), these basic indicators (requirements) are determined (clarified), taking into account the specifics and conditions of the functioning of the management system. Based on the proposed stages of evaluation of the software system, the article considers the main current scientific and methodological aspects of the application of proven methodological solutions in the field of quality assessment in the interests of improving (ensuring) the quality of software systems during operation. The definition of the methodology and possible directions of rational use are formulated. The methodology suggests improving the quality of software systems by making timely informed management decisions based on the results of evaluating the quality of software systems during operation. The article notes the practical orientation of the proposed methodology for improving the quality of software systems, due to the development and use of modern technologies, which provides prerequisites for increasing its versatility when using a large number of different software systems as part of interacting control systems for various purposes.*

Keywords: *quality assessment, system risk, software system, management decision, errors of the first and second kind.*

Information about Autors

Fortinsky A.G. – Candidate of Technical Sciences, Deputy General Director of TsNII EISU JSC. E-mail: cniieisu@cniieisu.ru. Tel.: +7 (495) 539-22-49. Address: Russia, Moscow, Malaya Bronnaya St., 2/7, page 1.

Bilyatdinov K.Z. – Candidate of Military Sciences, Associate Professor, Associate Professor of the Faculty of Infocommunication Technologies, ITMO National Research University. E-mail: od@mail.ifmo.ru. Tel.: +7 (812) 232-97-04. Address: Russia, St. Petersburg, Kronverksky Prospekt, d.49.

Spivak A.I. – Head of the Department of the Center for the Protection of State Secrets of the NCUO of the Ministry of Defense of the Russian Federation. E-mail: intelteh@inteltech.ru. Tel.: +7 (812) 313-12-51. Address: 197342, Russia, St. Petersburg, 8 Kantemirovskaya St.

Для цитирования: Фортинский А.Г., Билятдинов К.З., Спивак А.И. Об основах методологии повышения качества программных систем // Техника средств связи. 2021. № 2 (154). С. 81-85.

For citation: Fortinsky A.G., Bilyatdinov K.Z., Spivak A.I. On the basics of the methodology for improving the quality of software systems. Means of Communication Equipment. 2021. No. 2 (154). Pp. 81-85 (in Russian).

УДК 621.396

Обоснование выбора отечественной программной платформы управления ресурсами: инновации и оценка эффективности

Фортинский А.Г., Билятдинов К.З., Петров А.Н.

Аннотация: *Представленный в работе анализ показал, что эффективность любой сложной системы базируется на своевременном и обоснованном управленческом решении (действии), направленном на обеспечение (повышение) требуемой эффективности. Решение принимается по результатам оценки этой эффективности, как соотношение полученного результата и затраченных ресурсов, включая время достижения результата. Поэтому сегодня актуальной задачей является разработка и внедрение инновационного научно-методологического базиса оценки эффективности мероприятий (процедур) по обоснованию выбора отечественной программной платформы управления ресурсами. На данном базисе предлагаются инновационные основы научно-методологического подхода с применением модифицированного метода Data Envelopment Analysis для оценки эффективности процедур выбора отечественной программной платформы управления ресурсами. Инновации способствуют принятию управленческих решений по созданию условий для существенного снижения расхода ресурсов и времени на разработку и внедрение отечественной программной платформы. В статье приведено обоснование выбора отечественной программной платформы управления ресурсами. При этом анализ результатов научных исследований в предметной области выявил разнообразие мнений в этом вопросе и наличие ряда нерешенных задач в части рациональной организации оценки эффективности. В статье на основании научных работ М.Дж. Фаррелла в сфере развития методов непараметрического граничного анализа предлагается следующие направления применения модифицированного метода Data Envelopment Analysis: результативность (effectiveness) – определение степень достижения цели оцениваемой системой в заданный период времени; экономичность (efficiency) – это соотношение затрат ресурсов и результата, достигнутого оцениваемой системой в заданный период времени. Таким образом, в самом общем виде назначение модифицированного метода Data Envelopment Analysis в области оценки эффективности системы сводится к определению результативности и экономичности осуществляемого системой преобразования потребляемых ресурсов в получаемые результаты. Таким образом, в современных условиях всесторонний учет и сравнение результатов оценки эффективности различных процедур выбора позволит существенно расширить возможности создаваемой отечественной программной платформы.*

Ключевые слова: *модифицированный метод Data Envelopment Analysis, оценка эффективности, управление ресурсами, отечественная программная платформа.*

Актуальность

В настоящее время геополитические вызовы предопределяют необходимость повышения эффективности государственного управления. Отсюда возникает достаточно сильно выраженный научно-практический интерес к расширению оперативных возможностей органов государственной власти с минимальными затратами ресурсов и времени. В этой предметной области достижение высокой эффективности систем управления невозможно без создания высококачественной и эффективной отечественной программной платформы управления ресурсами.

Как известно, эффективность любой сложной системы базируется на своевременном и обоснованном управленческом решении (действии), направленном на обеспечение (повышение) требуемой эффективности. Решение принимается по результатам оценки этой эффективности, как соотношение полученного результата и затраченных ресурсов, включая время достижения результата [1, 2].

Поэтому сегодня актуальной задачей является разработка и внедрение инновационного научно-методологического базиса оценки эффективности мероприятий (процедур) по обоснованию выбора отечественной программной платформы управления ресурсами в интересах Федеральных органов исполнительной власти (далее – ФОИВ) для

информатизации их деятельности и перехода на импортозамещающие технологии, на примере Министерства обороны Российской Федерации, позволяющих проводить выбор платформы и прогнозирование соответствия перспективных платформ для управления ресурсами ФОИВ на этапе разработки.

В перспективе предлагаемые инновации будут применимы при системном подходе к рассмотрению и учету обеспечения эффективности целого ряда взаимосвязанных процессов, а именно выбора, разработки и внедрения отечественных программных продуктов.

Таким образом, к оценке эффективности процедур целесообразно подходить комплексно как оценке эффективности действий (решений) в сфере обоснования выбора, разработки и внедрения отечественной программной платформы.

Обоснование выбора отечественной программной платформы управления ресурсами

Инновации в сфере оценки эффективности прежде всего имеют целью обеспечение требуемого уровня качества отечественной программной платформы управления ресурсами.

Широкий спектр применения отечественной программной платформы управления ресурсами в ФОИВ, на предприятиях и в организациях, обосновывает введение допущения, что далее в настоящей статье мы будем использовать термин «система», понимая под ним в зависимости от условий постановки задачи оценивания как программный продукт, так и программную систему. Здесь важно заметить, что в соответствии с ГОСТ Р 51904-2002 «Программное обеспечение встроенных систем. Общие требования к разработке и документированию» программная система – это система, состоящая из программного обеспечения и компьютерного оборудования для его выполнения.

Итак, анализ результатов научных исследований в нашей предметной области выявил разнообразие мнений в этом вопросе и наличие ряда нерешенных задач в части рациональной организации оценки эффективности.

Результаты исследования, изложенные в работе [3], позволяют утверждать, что параллельный мониторинг неисправностей (отказов) элементов (изделий) в составе системы существенно повышает эффективность контроля эксплуатации.

В статье [4] отмечено, что учет специфики эксплуатации системы обеспечивает более рациональные эффективные подходы к планированию и обеспечению безопасности персонала.

Одновременно в научных работах [5-8] делается акцент на важность моделирования при принятии управленческих решений по результатам оценки эффективности [5] и для осуществления прогнозов на основе статистической информации об эксплуатации систем за прошедшие периоды времени [6] в интересах более эффективного использования инновационных возможностей информационных подсистем [7], а также по предупреждению и устранению неисправностей элементов в системе на этапе эксплуатации [8]. При этом в работах [9-12] обосновывается актуальность цели исследования для разработки новых подходов в области обеспечения эффективного и устойчивого функционированию систем [9], снижения риска системы при принятии управленческих решений [10].

В особенности это касается АСУ, а также важно и при решении задач их интеграции [8] в целях повышения эффективности управления.

Дополнительный дискурсивный анализ современных зарубежных научных исследований в сфере обеспечения безопасности, эффективности и устойчивости систем показывает ярко выраженную тенденцию расширения взглядов на применение результатов оценки эффективности систем при решении различных слабоструктурированных проблем управления:

в сфере идентификации отказов в автоматизированных системах;

при использовании в управлении информационных систем на основе математических моделей [13];

при оценке устойчивого развития и безопасности, включая оценку киберугроз для эксплуатируемых и разрабатываемых АСУ [14];

при применении систем искусственного интеллекта, больших данных и совершенствования систем управления с учетом современных направлений развития киберфизических систем [12-16].

Таким образом, результаты анализа научных исследований актуализуют и детализируют задачу нашего исследования в интересах повышения эффективности отечественной программной платформы управления ресурсами.

Дальнейший анализ в части касающейся оценки эффективности систем предполагает рассмотрение основ понятийного аппарата близкого к предметной области, предложенного О.Н. Моргуновой в научных работах [17, 18]. Качество сложной системы проявляется в полной мере только в процессе ее функционирования, т. е. при использовании по назначению. Поэтому наиболее объективная оценка качества системы может быть получена по эффективности ее целевого применения [17, 18].

По мнению Б.С. Флейшмана, «эффективность операции есть степень соответствия реального (фактического или ожидаемого) результата операции требуемому (желаемому) или, иными словами, степень достижения цели операции» [19].

Для выбранной предметной области исследования наиболее подходит следующее определение: «Эффективность – это наиболее общее, определяющее свойство любой целенаправленной деятельности, которое с познавательной (гносеологической) точки зрения раскрывается через категорию цели и объективно выражается степенью достижения цели с учетом затрат ресурсов и времени» [19].

При этом оценка эффективности систем будет неразрывно связана с понятием операции. Под операцией понимается упорядоченная совокупность взаимосвязанных действий, направленных на достижение определенной цели [20].

На основании данных работ в разрабатываемых методах и способах приоритетом оценки эффективности систем целесообразно считать оценку результативности и экономичности в процессе их эксплуатации по предназначению. Однако, рассмотренные результаты научных трудов, как и традиционные методы оценки качества напрямую не применимы для научно-методологического обеспечения разработки и внедрения комплекса новых научно обоснованных решений актуальной задачи исследования, вследствие особой специфики требований к отечественной программной платформе.

На практике оценка эффективности и качества систем может включать в себя следующие операции:

1) Сравнение показателей оцениваемой системы с показателями аналогичной системы, которая считается лучшей или, как вариант, с аналогичным системами.

2) Сравнение улучшения или ухудшения значений выбранных показателей одной системы за разные равные периоды времени, например, сравнение показателей за 2 квартал прошлого года и за 2 квартал текущего года и т. п.

3) Сравнение достигнутых значений выбранных показателей оценки с требуемыми значениями показателей, которые могут быть определены в различных нормативно-правовых актах, приказах (распоряжениях) руководствах, планах работы и т. д. [1, 2].

В исследуемой сфере объективная оценка эффективности систем требует подробной детализации и наиболее полного учета множества факторов и условий, которые сопровождают функционирование систем, а также их сравнение с аналогичными системами и (или) с различными периодами функционирования оцениваемых систем. Поэтому одним из перспективных направлений обеспечения достижения цели исследования является использование модифицированного метода *Data Envelopment Analysis* (*DEA*) [1, 2].

Для оценки качества системы любой природы важнейшей характеристикой является эффективность её функционирования. Однако очевидно, что никакой отдельный частный

показатель не может быть использован для универсального применения при оценке эффективности различных систем. Поэтому А. Чарнесом, В. Купером и Е. Родесом (A. Charnes, W. Cooper, E. Rhodes) был разработан метод «*Data Envelopment Analysis*» (*DEA*) или «Анализ среды функционирования» (АСФ), изложенный во многих научных работах [1, 2, 13].

В то же время применение метода *DEA* не дает объяснений причинам состояния системы и, соответственно, не дает дополнительной обоснованной информации для принятия наиболее рационального управленческого решения.

В предлагаемом модифицированном методе *DEA* устранены эти недостатки с помощью апробированных математических инструментов. Кроме того, предлагаемый метод в большей мере пригоден для программной реализации в силу использования систематизированных расчетных табличных форм.

Представляемый модифицированный метод *DEA* представляет собой симбиоз метода *DEA* («Анализа среды функционирования») и расчета корреляции зависимости [1, 2, 13].

На основании научных работ М.Дж. Фаррелла (*M.J. Farrell*) в сфере развития методов непараметрического граничного анализа можно сформулировать следующие направления применения модифицированного метода *DEA*:

1) Результативность (*effectiveness*) – определение степень достижения цели оцениваемой системой в заданный период времени.

2) Экономичность (*efficiency*) – соотношение затрат ресурсов и результата, достигнутого оцениваемой системой в заданный период времени.

Таким образом, в самом общем виде назначение модифицированного метода *DEA* в области оценки эффективности системы сводится к определению результативности и экономичности осуществляемого системой преобразования потребляемых ресурсов в получаемые результаты [1, 2].

При современном многообразии различных оцениваемых систем, выполняющих одинаковые функции, наиболее перспективным направлением применения модифицированного метода *DEA* будет являться первое направление, то есть оценка (сравнение) достигнутого результата с требуемым (базовым) значением этого результата за заданный период времени при условии одинаковых затрат ресурсов оцениваемыми системами.

Для этой цели в модифицированном методе *DEA* применяется парное сравнений количественных значений всех затраченных ресурсов и количественных значений достигнутого результата. Или сравнение достигнутого результата с его установленными базовыми (требуемыми) значениями. Проводятся сравнения всех оцениваемых систем и (или) оцениваемых периодов времени функционирования одной системы.

Ключевым моментом в модифицированном методе *DEA* является рекомендация по установлению базовых количественных значений для результата и затраченных ресурсов.

Систематизированная информация, полученная в результате расчетов, позволит лицу, принимающему решение, более детально провести анализ зависимостей ухудшения или улучшения значений корреляционной зависимости. Применение метода на практике может быть использовано для совершенствования управляющих воздействий, направленных на достижение цели функционирования системы.

По сути, разработанный модифицированный метод *DEA* – это инструмент бенчмаркинга. Бенчмаркинг позволяет определить наиболее эффективные подсистемы (элементы, изделия) в составе оцениваемой системы [1, 2, 13].

В идеале, при применении модифицированного метода *DEA* анализ зависимостей ухудшения или улучшения согласованности по различным оцениваемым событиям (вариантам решений), поможет выявить проблемы в процессе обоснования выбора отечественной аппаратной платформы и принять обоснованные решения по их исправлению.

Выводы

В заключении важно отметить, что в современных условиях всесторонний учет и сравнение результатов оценки эффективности различных процедур выбора позволит существенно расширить возможности создаваемой отечественной программной платформы, как важнейшей части системы импортозамещения в сфере высоких технологий, для наиболее рационального достижения целей повышения обороноспособности и безопасности Российской Федерации. Системное внедрение апробированных результатов современных научных исследований в сфере оценки эффективности сложных систем [1, 2] позволит усилить содержательный аспект процедур обоснования выбора отечественной программной платформы, что в итоге создаст условия для обеспечения требуемого уровня качества отечественных программных продуктов.

Литература

1. Билятдинов К.З., Меняйло В.В. Методика оценки эффективности систем на основе модифицированного метода DEA // Вестник воздушно-космической обороны, вып. 3, 2020. С. 66-74.

2. Билятдинов К.З., Меняйло В.В. Модифицированный метод DEA и методика оценки эффективности технических систем // Информационные технологии, вып. 11, 2020. С. 611-617.

3. Putz M., Wiene T., Pierer A. A multi-sensor approach for failure identification during production enabled by parallel datamonitoring. CIRP annals-manufacturing technology. 2018. Vol. 67. № 1. Pp. 491-494.

4. Golabchi A., Han S., AbouRizk S. A simulation and visualization-based framework of labor efficiency and safety analysis for prevention through design and planning. Automation in Construction. 2018. Vol. 96. Pp. 310-323.

5. Filz M., Herrmann C., Thiede S. Simulation-based Assessment of Quality Inspection Strategies on Manufacturing Systems. Procedia CIRP. 2020. Vol. 93. Pp. 777-782.

6. Hund L., Schroeder B., Rumsey K., Huerta G. Distinguishing between model- and data-driven inferences for high reliability statistical predictions. Reliability Engineering and System Safety. 2018. Vol. 180. Pp. 201-210.

7. Lumpkin D.R., Horton W.T., Sinfield J.V. Holistic synergy analysis for building subsystem performance and innovation opportunities. Building and Environment. 2020. Vol. 178. Article 106908.

8. Wang T., Qiao M., Zhang M. Data-driven prognostic method based on self-supervised learning approaches for fault detection. Journal of intelligent manufacturing. 2020. № 31(7). Pp. 1611-1619.

9. Calabrese R., Osmetti S.A. A new approach to measure systemic risk: A bivariate copula model for dependent censored data. European Journal of Operational Research. 2019. Vol. 279(3). Pp. 1053-1064.

10. Pačaiová H., Sinay J., Nagyová A. Development of GRAM – A risk measurement tool using risk based thinking principles. Measurement: Journal of the International Measurement Confederation. 2017. No. 100. Pp. 288-296.

11. Shafik M.B., Chen H., Rashed G. Planning and reliability assessment to integrate distributed automation system into distribution networks utilizing binary hybrid PSO and GSA algorithms considering uncertainties. International Transactions on Electrical Energy Systems. 2020. Article e12594.

12. Price M., Walker S., Wiley W. The Machine Beneath: Implications of Artificial Intelligence in Strategic Decision making. PRISM. 2018. Vol. 7. No. 4. Pp. 92-105.

13. Gerami J. An interactive procedure to improve estimate of value efficiency in DEA. Expert Systems with Applications. 2019. No. 137. Pp. 29-45.

14. Downes C. Strategic Blind–Spots on Cyber Threats, Vectors and Campaigns. The Cyber Defense Review. 2018. Vol. 3. No. 1. Pp. 79-104.

15. Baker J., Henderson S. The Cyber Data Science Process. The Cyber Defense Review. 2017. Vol. 2. No. 2. Pp. 47-68.

16. Trevino M. Cyber Physical Systems: The Coming Singularity. PRISM. 2019. Vol. 8. No. 3. Pp. 2-13.

17. Моргунова О. Н. Информационная система как источник данных для оценки уровня эффективности объектов и процессов в сфере высшего образования // VI Всероссийская научно-техническая конференция «Теоретические и прикладные вопросы современных информационных технологий», 25-31 июля 2005 г. (г. Улан-Удэ). Улан-Удэ: Изд-во ВСГТУ, 2005. Ч. 2. – С. 286-289.

18. Моргунова О. Н. Теория эффективности систем: некоторые вопросы и предложения // X Международная научно-практическая конференция «Системный анализ в проектировании и управлении». Санкт-Петербург. 2006. Ч. 1. – С. 119-122.

19. Флейшман Б.С. Основы системологии. – М.: Радио и связь, 1982. – 368 с.

20. Флейшман Б.С. Элементы теории потенциальной эффективности систем. – М.: Сов. радио, 1971. – 224 с.

References

1. Bilyatdinov K.Z., Menyaylo V.V. Methodology for assessing the effectiveness of systems based on the modified method DEA. Bulletin of Aerospace Defense, "Issue 3 (27), 2020. P. 66-74 (in Russian).

2. Bilyatdinov K.Z., Menyaylo V.V. Modified DEA method and methodology for evaluating the efficiency of technical systems. Information technologies, issue 11, 2020. P. 611-617 (in Russian).

3. Putz M., Wiene T., Pierer A. A multi-sensor approach for failure identification during production enabled by parallel datamonitoring. CIRP annals-manufacturing technology. 2018. Vol. 67. № 1. P. 491-494.

4. Golabchi A., Han S., AbouRizk S. A simulation and visualization-based framework of labor efficiency and safety analysis for prevention through design and planning. Automation in Construction. 2018. Vol. 96. P. 310-323.

5. Filz M., Herrmann C., Thiede S. Simulation-based Assessment of Quality Inspection Strategies on Manufacturing Systems. Procedia CIRP. 2020. Vol. 93. P. 777-782.

6. Hund L., Schroeder B., Rumsey K., Huerta G. Distinguishing between model- and data-driven inferences for high reliability statistical predictions. Reliability Engineering and System Safety. 2018. Vol. 180. P. 201-210.

7. Lumpkin D.R., Horton W.T., Sinfield J.V. Holistic synergy analysis for building subsystem performance and innovation opportunities. Building and Environment. 2020. Vol. 178. Article 106908.

8. Wang T., Qiao M., Zhang M. Data-driven prognostic method based on self -supervised learning approaches for fault detection. Journal of intelligent manufacturing. 2020. № 31(7). P. 1611-1619.

9. Calabrese R., Osmetti S.A. A new approach to measure systemic risk: A bivariate copula model for dependent censored data. European Journal of Operational Research. 2019. Vol. 279(3). P. 1053-1064.

10. Pačaiová H., Sinay J., Nagyová A. Development of GRAM – A risk measurement tool using risk based thinking principles. Measurement: Journal of the International Measurement Confederation. 2017. № 100. P. 288-296.

11. Shafik M.B., Chen H., Rashed G. Planning and reliability assessment to integrate distributed automation system into distribution networks utilizing binary hybrid PSO and GSA algorithms considering uncertainties. International Transactions on Electrical Energy Systems. 2020. Article e12594.

12. Price M., Walker S., Wiley W. The Machine Beneath: Implications of Artificial Intelligence in Strategic Decision making. PRISM. 2018. Vol. 7. No. 4. Pp. 92-105.

13. Gerami J. An interactive procedure to improve estimate of value efficiency in DEA. Expert Systems with Applications. 2019. № 137. P. 29-45.

14. Downes C. Strategic Blind–Spots on Cyber Threats, Vectors and Campaigns. The Cyber Defense Review. 2018. Vol. 3. No. 1. Pp. 79-104.

15. Baker J., Henderson S. The Cyber Data Science Process. The Cyber Defense Review. 2017. Vol. 2. No. 2. Pp. 47-68.

16. Trevino M. Cyber Physical Systems: The Coming Singularity. PRISM. 2019. Vol. 8. No. 3. Pp. 2-13.

17. Morgunova O.N. Information System as a data source for assessing the level of efficiency of objects and processes in the field of higher education.VI All-Russian Scientific and Technical Conference "Theoretical and Applied Issues of Modern Information Technologies," July 25-31, 2005 (Ulan-Ude). Ulan-Ude: Publishing House of VSSTU, 2005. Part 2. P. 286-289 (in Russian).

18. Morgunova O.N. Theory of System Efficiency: Some Questions and Suggestions//X International Scientific and Practical Conference "System Analysis in Design and Management." St. Petersburg. 2006. Part 1. P. 119-122 (in Russian).

19. Fleischmann B.S. Fundamentals of Systemology. Moscow. Radio and communications, 1982. 368 p. (in Russian).

20. Fleischmann B.S. Elements of the theory of potential efficiency of systems. Moscow. Sov. radio, 1971. 224 p. (in Russian).

Статья поступила 12 мая 2021 г.

Информация об авторах

Фортинский А.Г. – Кандидат технических наук, заместитель генерального директора АО «ЦНИИ ЭИСУ». E-mail: cniieisu@cniieisu.ru. Тел.: +7 (495) 539-22-49. Адрес: Россия, г. Москва, ул. Малая Бронная, д. 2/7, стр.1.

Билятдинов К.З. – Кандидат военных наук, доцент, доцент факультета инфокоммуникационных технологий Национальный исследовательский университет ИТМО. E-mail: od@mail.ifmo.ru. Тел.: +7 (812) 232-97-04. Адрес: Россия, г. Санкт-Петербург, Кронверкский пр-кт, д.49.

Петров А.Н. – Начальник отдела ПАО «Интелтех». E-mail: intelteh@inteltech.ru. Тел.: +7 (812) 313-12-51. Адрес: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

Substantiation of domestic software platform selection resource management: innovation and performance assessment

A.G. Fortinsky, K.Z. Bilyatdinov, A.N. Petrov

Abstract. *The analysis presented in the paper showed that the effectiveness of any complex system is based on a timely and reasonable management decision (action) aimed at ensuring (improving) the required efficiency. The decision is made based on the results of the evaluation of this efficiency, as the ratio of the result obtained and the resources spent, including the time to achieve the result. Therefore, today an urgent task is to develop and implement an innovative scientific and methodological basis for evaluating the effectiveness of measures (procedures) to justify the choice of a domestic resource management software platform. On this basis, we propose innovative foundations of a scientific and methodological approach using a modified Data Envelope Analysis method to assess the effectiveness of procedures for selecting a domestic resource management software platform. Innovations contribute to the adoption of management decisions to create conditions for a significant reduction in the consumption of resources and time for the development and implementation of a domestic software platform. The article provides a justification for the choice of a domestic software platform for resource management. At the same time, the analysis of the results of scientific research in the subject area revealed a variety of opinions on this issue and the presence of a number of unsolved problems in terms of the rational organization of efficiency assessment. In the article, based on the scientific works of M. J. In the field of development of methods of nonparametric boundary analysis, the following directions of application of the modified Data Envelope Analysis method are proposed: effectiveness-determining the degree of achievement of the goal by the evaluated system in a given period of time; efficiency is the ratio of resource costs and the result achieved by the evaluated system in a given period of time. Thus, in the most general form, the purpose of the modified Data Envelope Analysis method in the field of evaluating the effectiveness of the system is to determine the effectiveness and efficiency of the conversion of consumed resources into the results obtained by the system. Thus, in modern conditions, a comprehensive accounting and comparison of the results of evaluating the effectiveness of various selection procedures will significantly expand the capabilities of the domestic software platform being created.*

Keywords: *modified Data Envelope Analysis method, efficiency assessment, resource management, domestic software platform.*

Information about Autor

Fortinsky A.G. – Candidate of Technical Sciences, Deputy General Director of JSC TsNII EISU. E-mail: cniieisu@cniieisu.ru. Тел.: +7 (495) 539-22-49. Address: Russia, Moscow, ul. Malaya Bronnaya, d. 2/7, p. 1.

Bilyatdinov K. Z. – Candidate of Military Sciences, Associate Professor, Associate Professor, Faculty of Infocommunication Technologies, ITMO National Research University. E-mail: od@mail.ifmo.ru. Тел.: +7 (812) 232-97-04. Address: Russia, St. Petersburg, Kronverksky Prospekt, 49.

Petrov A.N. – Head of Department of PJSC «Inteltech». E-mail: intelteh@inteltech.ru. Тел.: +7 (812) 313-12-51. Address: 197342, Russia, St. Petersburg, 8 Kantemirovskaya St.

Для цитирования: Фортинский А.Г., Билятдинов К.З., Петров А.Н. Обоснование выбора отечественной программной платформы управления ресурсами: инновации и оценка эффективности // Техника средств связи. 2021. № 2 (154). С. 86-92.

For citation: Fortinsky A.G., Bilyatdinov K.Z., Petrov A.N. Substantiation of domestic software platform selection resource management: innovation and performance assessment. Means of Communication Equipment. 2021. No. 2 (154). Pp. 86-92 (in Russian).

ОБЪЕКТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ И ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ОБЛАСТИ РАЗРАБОТКИ СРЕДСТВ ТЕЛЕКОММУНИКАЦИЙ

УДК 378.016

Разработка интерактивного электронного руководства

Крымская С.А.

Аннотация: *в статье рассматривается проект по разработке интерактивного электронного руководства на Изделия. Цель: совершенствование системы подготовки специалистов к эксплуатации Изделий в условиях учебных центров и войсковых частей, внедрение интерактивного электронного руководства как эффективной альтернативы документации на бумажных носителях.*

Ключевые слова: *интерактивное электронное руководство, электронная документация, эксплуатационная документация, учебно-тренировочные средства, программно-методический комплекс.*

Введение

В настоящее время развитие *IT*-технологий активно внедряется во все сферы жизнедеятельности. Разработка сложных комплексов связи подразумевает более длительный и сложный процесс подготовки персонала к работе с Изделиями, а также большой объем документации на Изделие, что в свою очередь усложняет процесс разработки и эксплуатации технических средств на всех этапах реализации. Внедрение интерактивного электронного руководства (ИЭР) в жизненный цикл процесса разработки и эксплуатации Изделия как неотъемлемую часть информационно-технического сопровождения предполагает облегчение процесса обучения и подготовки персонала к работе с Изделием в боевых условиях, а также существенно упрощает процесс сопровождения Изделия, начиная с этапа разработки и до ввода в эксплуатацию на местах дислокации. На текущий момент нет единых требований к информационно-техническому сопровождению разрабатываемых Изделий, несмотря на общую тенденцию развития процессов информатизации. К тому же, в условиях увеличения сложности и многозадачности разрабатываемых технических средств, что влечет за собой значительное увеличение объема документации, вопрос структуризации и быстрого доступа к информации становится более актуальным. *Целью разработки* ИЭР является совершенствование системы подготовки персонала к эксплуатации Изделий, средствами информационных технологий.

Основной функцией ИЭР является организация взаимосвязи текстовой информации и интерактивных иллюстраций с использованием гиперссылок, создавая мощный интерактивный документ, подкрепленный чертежами, рисунками, фото- и видео материалом, интерактивными схемами, *3D* – моделями, комплексными *Flash*-анимациями. ИЭР позволяет предоставить персоналу непосредственно на рабочем месте быстрый доступ к технической и эксплуатационной документации на Изделие, обеспечить возможность оперативного поиска необходимой для работы информации, своевременного внесения изменений в документацию, а также повышение уровня осведомленности о работе с Изделием. С учетом этого возникает потребность в создании механизма, структурирующего массив информации с минимальными временными и материальными затратами.

1. Постановка задачи на разработку интерактивного электронного руководства

Интерактивные электронные руководства применяются для решения широкого спектра задач: обеспечение справочным материалом об устройстве и принципах работы Изделия (в виде электронных документов с элементами мультимедиа); обеспечение персонала справочным материалом при использовании Изделия по назначению; обеспечение справочным материалом при техническом обслуживании и ремонте Изделия; обеспечение персонала информацией о проведении технологических операций с Изделием (необходимый инструмент и материалы, количество и квалификация персонала); оперативный интеллектуальный поиск необходимой информации об Изделии; автоматизированный сбор, хранение и обработка данных, полученных с диагностических приборов; мониторинг технического состояния оборудования, поиск и выявление причин неисправностей, выдача рекомендаций по их устранению; планирование и учет проведения регламентных работ; автоматизированный заказ материалов и запасных частей; накопление полученных в процессе эксплуатации технических данных, их анализ и выдача рекомендаций пользователям по дальнейшей эксплуатации Изделия; обучение персонала правилам использования, обслуживания и ремонта Изделия, проведение занятий по специальности; тренировка

персонала по использованию Изделия в нормальных и аварийных ситуациях; тестирование персонала на предмет допуска к самостоятельной эксплуатации Изделия. ИЭР может включать в себя интегрированную базу данных (БД) и знаний (БЗ), где хранится информация об Изделии, а также электронную систему отображения для визуализации данных и обеспечения интерактивного взаимодействия с персоналом.

2. Используемые методы разработки интерактивного электронного руководства

На сегодня в каждой воинской части и подразделениях имеются ЭВМ, используемые в учебных целях. Это позволяет полноценно внедрять и использовать ИЭР непосредственно на местах эксплуатации технических средств. Информационное наполнение ИЭР происходит на стадиях разработки и производства Изделия и поставляется вместе с документацией на Изделие на электронном носителе. ИЭР подразумевает минимальный набор требований для функционирования – наличие ЭВМ с установленной операционной системой (ОС), запускается с помощью ее стандартного *WEB*-браузера и не требует специальной установки. А для работы с ИЭР достаточно базовых знаний персонального компьютера.

При разработке ИЭР используется любой *HTML*-редактор с возможностью внедрения *JavaScript*-кода, вставки таблиц в текстовый блок, возможностью использования графических данных (видео файлов), а также организации интерактивной связи между графическим материалом (в том числе и *3D*-моделями) и текстом.

Для разработки ИЭР могут использоваться следующие языки программирования: *HTML, JavaScript, CSS*. Использование *HTML*-языка для создания ИЭР имеет ряд преимуществ. *HTML* позволяет создавать *WEB*-страницы, добавляя мультимедийные контенты, не используя дополнительных программ. Так же с помощью *HTML* можно разработать пользовательский интерфейс, максимально удобным для эксплуатации персоналом.

3. Архитектура построения интерактивного электронного руководства

С позиции разработчика ИЭР удобно за счет использования единого источника данных. Документация на Изделие или комплекс Изделий, а также учебно-тренировочные средства объединены в общий массив, который можно разделить на несколько модулей:

«Основные этапы и последовательность выполнения технологических операций подготовки Изделия для эксплуатации», с обеспечением в интерактивном режиме демонстрации и изучения основных этапов подготовки Изделия;

«Подготовка средств технологического оснащения», с обеспечением в интерактивном режиме демонстрации и изучения основных этапов подготовки средств технологического оснащения;

«Имитация нештатных ситуаций» содержит перечнем возможных нештатных и аварийных ситуаций, а также с обеспечением в интерактивном режиме демонстрации их развития их последствий;

«Функционирование систем и составных частей Изделия», с обеспечением в интерактивном режиме демонстрации и изучения функционирования основных систем и составных частей Изделия;

«Состав и основные требования эксплуатационной документации, регламентирующей подготовку Изделия к эксплуатации». Обеспечивает в интерактивном режиме изучение состава и основных требований эксплуатационной документации, описывающей подготовку Изделия к работе.

«Информационное ядро» является основным информационным хранилищем учебно-тренировочного программно-методического комплекса, необходимого для функционирования всех модулей и подсистем ИЭР. Включает электронные модели Изделия, процессов, технологической системы, нормативно-техническую документацию, представленную в электронном виде;

«Обслуживание информационного ядра», с обеспечением возможности ввода принципиально новой (дополнительной) и редактирования уже занесенной в информационное ядро информации по Изделию (модернизация, варианты исполнения), процессам функционирования основных систем, содержанию этапов подготовки, средств технологического оснащения Изделия.

Пример структурирования и наполнения информационной базы ИЭР показан на рис. 1.

При разработке ИЭР важной целью является объединить сведения, требующиеся для эксплуатации, как самого Изделия, так и его составных частей. Для этого организовывается структуризация документов по разделам и по тематике основного Изделия и составных частей. За основу структуры будущего ИЭР необходимо взять руководство по эксплуатации (РЭ) Изделия. После чего требуется объединить по смыслу разделы основного РЭ Изделия с разделами других эксплуатационных документов на это же Изделие используя перекрестные ссылки из руководства с возможностью перехода на схожие по тематике разделы других документов и обратно.

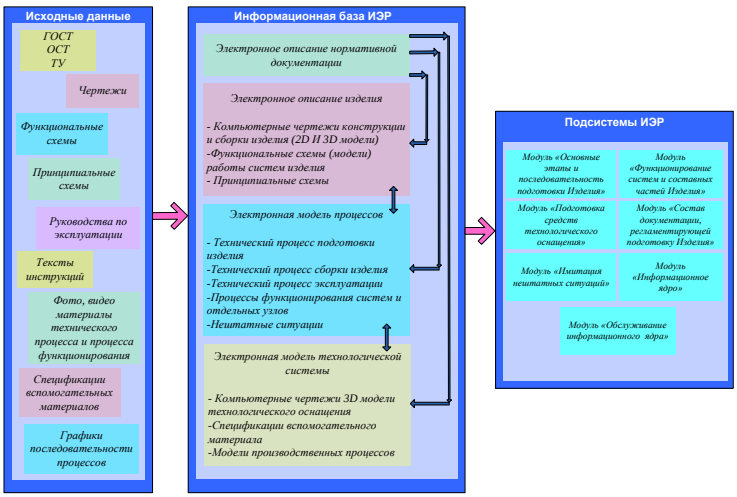


Рис. 1. Структура разработки и наполнения информационной базы ИЭР

При объединении разделов можно использовать разный подход. Включить в состав структуры разделов основного РЭ разделы других документов. Допустим, в РЭ есть раздел «Хранение и транспортирование». К данному разделу по смыслу близок документ «Инструкция по хранению и транспортированию». Объединить информацию можно, взяв структуру раздела «Инструкции по хранению и транспортированию» включив их подразделами в раздел «Хранение и транспортирование».

Возможно включать в состав структуры разделов основного руководства по эксплуатации целые документы. Например, в выбранном нами руководстве по эксплуатации есть раздел «Средства измерения, инструмент и принадлежности». Данному разделу соответствует по смыслу документ «Ведомость ЗИП». Поскольку сам документ «Ведомость ЗИП» на разделы не разбит, его можно включить как модуль данных в состав раздела «Средства измерения, инструмент и принадлежности».

Можно объединить сведения из разделов основного руководства по эксплуатации со сведениями из разделов других документов. Например, в руководстве по эксплуатации есть раздел «Технические характеристики». Этот раздел по смыслу соответствует разделу «Основные сведения об Изделии и технические данные» из документа «Паспорт». В результате можно объединить информацию из двух документов в один раздел основного РЭ. Способы объединения комплекта эксплуатационных документов, выполненных по ГОСТ, представлены на рис. 2.

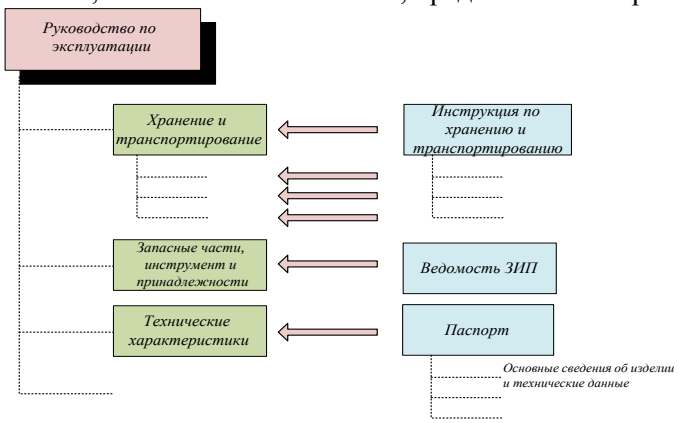


Рис. 2. Пример объединения комплекта эксплуатационной документации в единый документ

Так же объединяются разделы основного руководства по эксплуатации, посвященные составным частям Изделия, с комплектом документов на эти же составные части. К примеру, в РЭ Изделия есть раздел «Описание и работа». В нем имеется два подраздела – «Описание и работа Изделия» и «Описание и работа составных частей Изделия». В разделе «Описание и работа Изделия» дается информация об Изделии в целом, а раздел «Описание и работа составных частей Изделия» можно структурировать, разделив по наименованию составных частей, и в каждом таком подразделе привести сведения из основного РЭ об этой составной части. Аналогичный подход можно применить в разделе «Техническое обслуживание» из основного РЭ. В разделах, где информация о составных частях не предусмотрена, необходимо ее ввести. Например, разделы «Хранение»,

«Транспортирование», «Утилизация» основного РЭ не содержат информации о составных частях, поэтому необходимо ввести в каждом из этих разделов два подраздела: «Хранение Изделия» и «Хранение составных частей Изделия», «Транспортирование Изделия» и «Транспортирование составных частей Изделия», «Утилизация Изделия» и «Утилизация составных частей Изделия».

Структурировать информацию в ИЭР необходимо также с учетом применения как в режимах обучения персонала работе с Изделием, так и в условиях боевых дежурств на местах непосредственной эксплуатации Изделия. На рис. 3 наглядно показано, как организована работа структурированной информации в виде ИЭР, например, в обучающих центрах, на полигонах и в ходе боевого дежурства.

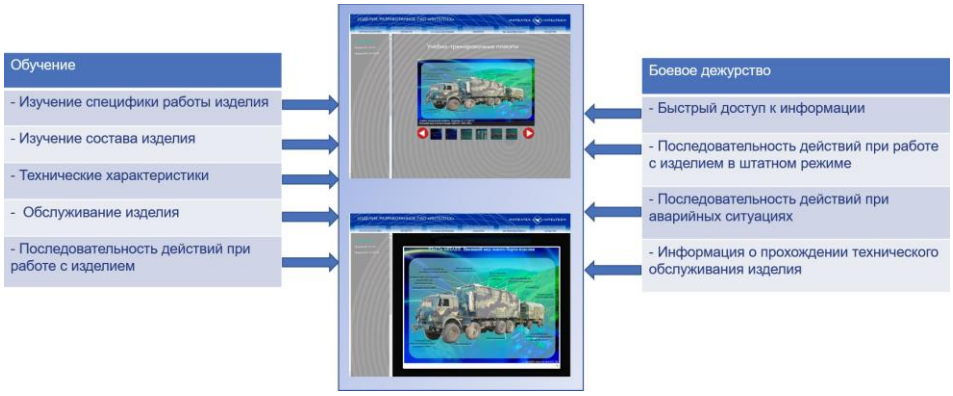


Рис. 3. Пример работы с ИЭР в режиме обучения и боевого дежурства

Немаловажно разработать эргономичный интерфейс ИЭР, где информация будет доступна в удобном формате. Пример классического расположения древовидного меню и выводом основной текстовой информации в главный блок с перекрестными ссылками показан на рис. 4.

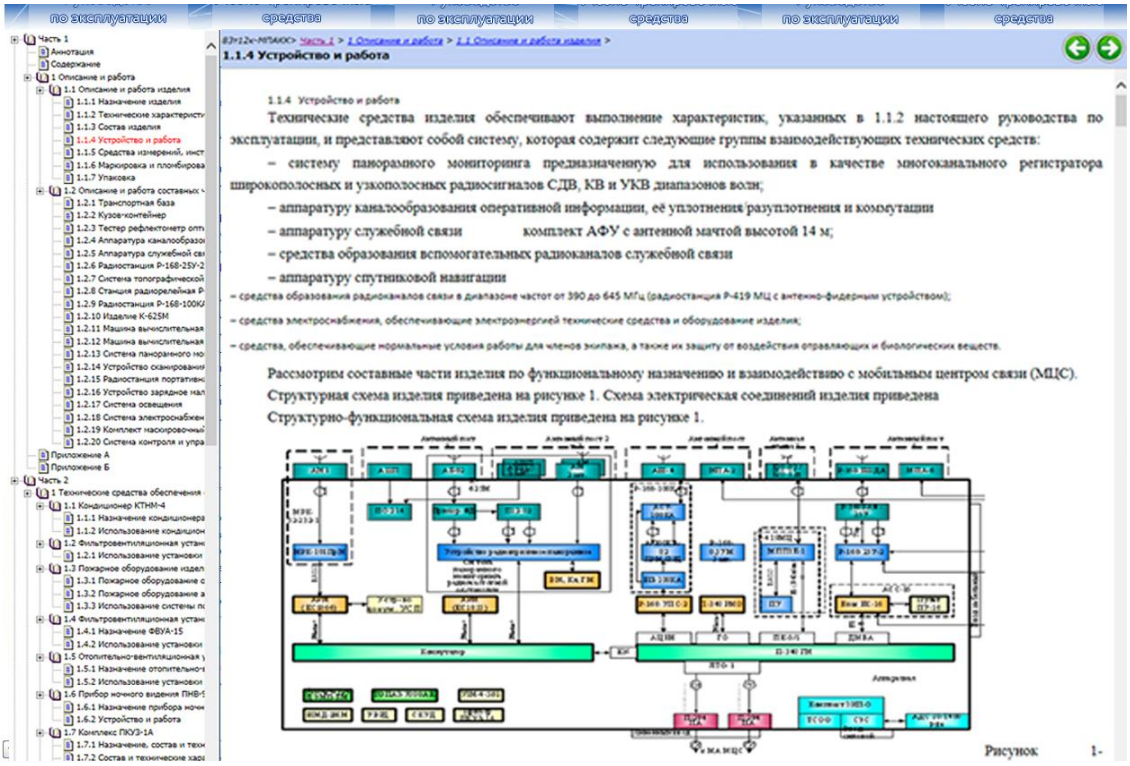


Рис. 4. Оформление интерфейса ИЭР

Демонстрация мультимедийных элементов – схем, плакатов, обучающих видеороликов также выводится в главный информационный блок ИЭР (рис. 5). Такая компиляция информации ИЭР наиболее эргономична для эксплуатации пользователем.

Таким образом, используя подобную систему структуризации документации, можно создать удобный и доступный механизм для освоения, изучения сложных технических средств, повышения качества навыков работы с Изделием.

Рис. 5. Демонстрация учебно-тренировочных плакатов

4. Классификация интерактивных электронных руководств

В зависимости от функциональности ИЭР, их подразделяют на 5 классов сложности в соответствии с ГОСТ Р 54088-2010:

1-й класс – Бумажно-ориентированные электронные документы. Они предполагают перевод бумажных руководств в электронный вид простым сканированием изображений и снабжением их кратким оглавлением. Основной целью при переводе бумажных руководств в электронный вид является преобразование нескольких килограмм бумаги в маленький электронный носитель. Страницы индексированы в соответствии с содержанием, перечнем иллюстраций, таблиц и т. п. Индексация позволяет отобразить растровое представление раздела документации сразу после его выбора в содержании ИЭР. Этот вид ИЭР сохраняет ориентированность страниц, которые могут быть выведены на печать без предварительной обработки.

2-й класс – Неструктурированные документы. При их создании отсканированные страницы руководств необходимо распознать – это позволит работать с данными, представленными в виде текста. К этому классу можно отнести электронные документы, выполненные в формате *HTML*. ИЭР второго класса позволяет расширить функции бумажных руководств за счет добавления к ним новых возможностей: ссылок для автоматического перехода из любого места документа в другое. Как правило, ИЭР этого класса позволяют производить поиск данных, могут содержать растровую и/или векторную графику, сноски и заметки. ИЭР этого класса может быть просмотрена на экране и выведена на печать без предварительной обработки.

3-й класс – Структурированные документы. Основным преимуществом является возможность стандартизации. ИЭР, в которых технические данные представлены в виде совокупности взаимосвязанных информационных объектов, хранящихся в БД и имеющих иерархическую структуру (в соответствии с требованиями международных стандартов и производных от него спецификаций).

4-й класс – Интерактивные базы данных. В отличии от третьего класса, представляющего собой набор файлов, ИЭР 4 класса для хранения информации применяется промышленная система управления БД, что позволяет эффективно управлять большими объемами данных и, соответственно, создавать и использовать ИЭР на сложные промышленные Изделия. Кроме того, исключение дублирования многократно использующихся данных приводит к значительному уменьшению объема документации и вероятности ошибки при повторном вводе идентичной информации. ИЭР этого класса позволяют анализировать состояние Изделия в конкретной ситуации, в том числе проводить операции поиска отказов и неисправностей в Изделии, определение причин сбоев, подбора запасных частей и т. д.

5-й класс – ИЭР, обладающие основной функциональностью предыдущих классов и включающие в себя средства накопления полученных в процессе эксплуатации технических данных, их анализа и формирования рекомендаций пользователям ИЭР о предпочтительном порядке обслуживания Изделия и диагностики неисправностей.

Вывод

В настоящее время, при усложнении функционала технических средств и растущем объеме информации, актуальной является задача структуризации и доступности информации для обслуживающего персонала, а также разработчиков на разных этапах разработки Изделий. Это возможно осуществить с помощью внедрения в жизненный цикл Изделия разработки интерактивного электронного руководства, что позволит существенно облегчить процесс эксплуатации Изделия на всех этапах функционирования. При освоении нового Изделия применение ИЭР позволяет на 20-25 % сократить сроки обучения. При этом существенно повышается средний уровень освоения материала. Одно интегрированное ИЭР может заменить собой целый комплекс традиционных технических руководств по эксплуатации, техническому обслуживанию и ремонту Изделия. В интегрированном ИЭР организовать обновление информации гораздо проще, чем в бумажных руководствах.

Литература

1. ГОСТ Р 54088 – 2017. Интегрированная логистическая поддержка. Эксплуатационная и ремонтная документация в форме интерактивных электронных технических руководств. – М.: Стандартинформ, 2018. – 12 с.

2. ГОСТ Р 54089 –2018. Интегрированная логистическая поддержка. Электронное дело изделия. Основные положения и общие требования. – М.: Стандартинформ, 2018. – 11 с.

3. Теоретические основы автоматизированных систем обучения. / Под ред. В.В. Могулина. – М.: МО, 1989. – 254 с.

4. Корнеев И.К., Машурцев В.А. Информационные технологии в управлении. – М.: ИНФРА-М, 2001. – 158 с.

References

1. GOST R 54088 2017. Integrated logistics support. Maintenance and repair documentation in the form of online electronic technical manuals. Moscow. Standardized Publ., 2018. 12 p. (in Russian).

2. GOST R 54089 2018. Integrated logistics support. Electronic product case. Main provisions and general requirements. Moscow. Standardized Publ., 2018. 11 p. (in Russian).

3. Theoretical foundations of automated training systems. Ed. V.V. Mogulin. Moscow. MO, 1989. 254 p. (in Russian).

4. Korneev I.K., Mashurtsev V.A. Information technology in management. Moscow. INFRA-M Publ., 2009. 224 p. (in Russian).

Статья поступила 15 марта 2021 г.

Информация об авторе

Крымская Светлана Аркадьевна – Инженер 2 категории ПАО «Интелтех». E-mail: krymskaya.sa@gmail.com. Адрес: 197342, Россия, Санкт-Петербург, Кантемировская, 8.

Development of an interactive e-guide

Krymskaya S.A.

Abstract. *The article discusses a project for the development of an interactive electronic manual for Products. Objective: to improve the system of training specialists for the operation of Products in the conditions of training centers and military units, the introduction of an interactive electronic manual as an effective alternative to paper documentation.*

Keywords: *interactive electronic manual, electronic documentation, operational documentation, training tools, software and methodological complex.*

Information about Authors

Krymskaya Svetlana Arkadyevna – Engineer of the 2nd category of PJSC «Inteltech». E-mail: krymskaya.sa@gmail.com. Address: 197342, Russia, St. Petersburg, st. Kantemirovskaya, 8.

Для цитирования: Крымская С.А. Разработка интерактивного электронного руководства // Техника средств связи. 2021. № 2 (154). С. 93-98.

For citation: Krymskaya S.A. Development of an interactive e-guide. Means of communication equipment. 2021. No 2 (154). P. 93-98 (in Russian).

О журнале «Техника средств связи»
«Means of Communication Equipment»

Научно-технический журнал «Техника средств связи» (переводное издание «Means of Communication Equipment») – это рецензируемое научное издание, в котором публикуются результаты научных исследований специалистов в области современных инфокоммуникационных технологий и автоматизированных систем управления, средств связи и информационной безопасности.

Журнал является правопреемником издававшихся с 1959 года Министерством промышленности средств связи СССР всесоюзных журналов «Вопросы радиоэлектроники. Серия: Техника проводной связи» и «Вопросы специальной радиоэлектроники. Серия: Техника проводной связи». С 1975 года журнал издается под названием «Техника средств связи».

Учредитель и издатель журнала: Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»). Адрес учредителя и издателя журнала: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

Периодичность выхода журнала 4 номера в год (очередные номера выходят ежегодно – 20 марта, 20 июня, 20 сентября и 20 декабря).

Публикация в журнале является научным печатным трудом. Основное содержание издания представляют собой научные статьи и научные обзоры.

Информация предназначена для детей старше 12 лет.

Журнал зарегистрирован как сетевое и печатное издания в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Свидетельства о регистрации средств массовой информации:
ПИ № ФС 77 – 80135 от 31.12.2020 г.
ЭЛ № ФС 77 – 80136 от 31.12.2020 г.
ISSN (print): 2782-2141
ISSN (online): 2782-2133

Перечень научных специальностей, паспорта которых соответствуют тематическому содержанию журнала

05.00.00 – Технические науки	*05.12.00 «Радиотехника и связь»*
	05.12.04 «Радиотехника, в том числе системы и устройства телевидения»
	05.12.07 «Антенны, СВЧ устройства и их технологии»
	05.12.13 «Системы, сети и устройства телекоммуникаций»
	05.13.00 «Информатика, вычислительная техника и управление»
	05.13.01 «Системный анализ, управление и обработка информации»
	05.13.05 «Элементы и устройства вычислительной техники и систем управления»
	05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»
	05.13.15 «Вычислительные машины, комплексы и компьютерные сети»
	05.13.18 «Математическое моделирование, численные методы и комплексы программ»
	05.13.19 «Методы и системы защиты информации, информационная безопасность»
20.00.00 – Военные науки	20.01.09 «Военные системы управления, связи и навигации»
	20.01.10 «Военная разведка»
	20.01.12 «Радиоэлектронная борьба (способы и средства)»
	20.02.12 «Системный анализ, моделирование боевых действий и систем военного назначения, компьютерные технологии в военном деле»
	20.02.14 «Вооружение и военная техника. Комплексы и системы военного назначения»
	20.02.17 «Эксплуатация и восстановление вооружения, техническое обеспечение»
	20.02.25 «Военная электроника, аппаратура комплексов военного назначения»