ПРЕДЛОЖЕНИЯ ПО МОДЕРНИЗАЦИИ ПРОТОКОЛА МОНИТОРИНГА ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ УЗЛА СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Боговик А.В.[1], Сафиулов Д.М.[2]

DOI:10.21681/3034-4050-2025-2-53-64

Ключевые слова: *удаленная диагностика, адаптивный сбор данных, иерархические структуры MIB (Management Information Base), полевые условия, радиоэлектронное противодействие, надежность каналов, интеллектуальная конфигурация, гибкая детализация*

Аннотация

Целью *статьи является анализ существующих методов сбора и обработки данных о состоянии телекоммуникационного оборудования сетей связи специального назначения и разработка предложений по реализации удаленной адаптивной диагностики, учитывающей особенности полевых условий и высокие требования к скрытности.*

Методы *исследования заключаются в использовании механизмов сравнительного анализа в процессе управления сетевыми устройствами, формализованных моделей полноты информации и алгоритмов необходимого покрытия для оптимизации структуры набора применяемых датчиков. В качестве методологической основы послужили труды по повышению устойчивости сенсорных сетей в условиях ограничения ресурсов, проведены моделирование и экспертная оценка, позволившие выявить ключевые показатели эффективности предложенного подхода.*

Результаты *исследования. В ходе работы проанализированы проблемы, возникающие при эксплуатации узлов связи в условиях ограниченной пропускной способности каналов и высокого риска радиоэлектронного противодействия. Показано, что стандартный механизм удаленного мониторинга, предусматривающий постоянную детализацию и равномерную частоту опроса, в боевой обстановке приводит к избыточному объему служебного трафика и может демаскировать важные элементы инфраструктуры. Разработанная стратегия позволяет динамически менять глубину диагностирования и интервалы получения данных, избегая перегрузки сетевых ресурсов. Это достигается благодаря дополнению библиотеки параметров MIB новыми идентификаторами и Trap-сообщениями, которые активируются только при выявлении угроз или отклонений от нормальных режимов работы. Предложенный подход значительно сокращает время обнаружения неисправностей, повышает оперативность их устранения и уменьшает риск потери критической информации, что крайне важно для полевых систем военного назначения и сопряженных с ними узлов связи. Кроме того, детально рассмотрены алгоритмы адаптивной частоты опроса, позволяющие снизить нагрузку в периоды стабильной работы и немедленно повысить чувствительность мониторинга при возникновении нештатных ситуаций. Такая гибкость обеспечивает как эффективную диагностику, так и необходимый уровень скрытности.*

Научная новизна *работы заключается в предложении формальных моделей, основанных на эффективной полноте данных и задачах покрытия, позволяющих количественно обосновывать выбор глубины мониторинга и частоты опроса. Введение новых идентификаторов и сообщений в MIB раскрывает дополнительные возможности для интеллектуальной перенастройки агентов мониторинга с учетом динамики обстановки и ограниченных ресурсов канала.*

Введение

Современные системы мониторинга телекоммуникационного оборудования в основном проектировались для стационарных сетей с высокой пропускной способностью. Однако в ходе современных операций каналы связи работают в условиях дефицита пропускной способности, а интенсивное огневое и радиоэлектронное противодействие серьезно затрудняет их стабильное функционирование. Как отмечается в [1, 2, 3], необходимость оперативного предоставления услуг связи органам военного управления часто приводит к несбалансированным настройкам протоколов маршрутизации, параметров *QoS* (набор

[1]Боговик Александр Владимирович, кандидат военных наук, профессор, профессор кафедры Военной академии связи, г. Санкт-Петербург, Россия. E-mail: bogovikav@mail.ru

[2]Сафиулов Давлет Муратович, адъюнкт Военной академии связи, г. Санкт-Петербург, Россия. E mail: davletzas@mail.ru

технологических решений *Quality of Service*) и других сервисных механизмов, а экстремальные климатические факторы и нестабильное энергоснабжение от полевых генераторов провоцируют систематические аномалии, сбои и отказы телекоммуникационного оборудования (ТКО). Особенно это чувствительно для средств связи критичной номенклатуры, качество функционирования которых напрямую влияет на выполнение оперативных задач управления войсками и оружием[3] [2]. В связи с этим обеспечение более качественного мониторинга технического состояния ТКО становится приоритетной задачей для систем управления связью, требующей внедрения модульных механизмов контроля параметров, таких как динамическая адаптация частоты опроса и глубины диагностирования. Реализация эффективного протокола мониторинга, интегрированного с возможностями адаптивного управления, может стать решением вопросов отказоустойчивости и оперативности систем связи в условиях ограниченных ресурсов и деструктивных воздействий.

Классический протокол мониторинга *SNMP* (*Simple Network Management Protocol*), основанный на механизме «менеджер-агент» и операциях *Get/Set/Trap/Inform* [3], широко используется в составе различных систем, включая решения на базе специального программного обеспечения наподобие *Zabbix* (по результатам проведённого анализа [4], это одна из наиболее распространённых реализаций). Однако традиционная спецификация *SNMP* не предусматривает гибкого изменения глубины мониторинга и частоты опроса. При низкоскоростных каналах и высоком риске потерь подробный мониторинг перегружает сеть, однако в критические моменты требуется немедленная детальная информация о состоянии эксплуатируемых объектах на узлах связи. Так возникает противоречие: нужно минимизировать трафик в штатном режиме и уметь быстро повышать полноту данных при обнаружении существенных аномалий в работе ТКО и/или падения качества услуг связи.

Актуальность модернизации простого протокола мониторинга *SNMP* обусловлена необходимостью динамически выбирать степень детализации и частоту опроса, что позволяет экономить ресурсы при нормальных условиях и оперативно наращивать объем собираемой информации в случае угроз. В настоящей статье обосновывается возможность такого подхода, предлагаются механизмы расширения библиотеки параметров *MIB* (*Management Information Base*) и описываются сценарии внедрения, ориентированные на узлы связи специального назначения.

Постановка задачи

Требуется разработать и формально обосновать расширенный вариант протокола мониторинга SNMP, предназначенный для управления состоянием ТКО узлов связи в полевых условиях с ограниченной полосой пропускания и высоким риском деструктивных воздействий. Предполагается дополнить стандартные операции (*Get, Set, GetNext, Trap, Inform*) механизмами динамического управления глубиной диагностики (τ) (через *OID* типа *oidDetailLevel*) и частотой опроса (f) (через *oidSamplingFreq*).

Для формализации возникающего компромисса используются положения теории достаточной статистики [5], согласно которым эффективность диагностики возрастает по мере увеличения полноты данных, но избыточное количество и слишком частый сбор информации перегружают сеть и замедляют анализ. Пусть $U_{эфф}(\tau,f)$ — эффективная полнота информации, достигаемая при выбранных τ и f. Тогда время диагностики отказа $T_{диагн}$ можно оценивать через рациональную аппроксимацию:

$$T_{диагн}(\tau,f)=\frac{1}{1+\alpha\cdot\dfrac{U_{\min}}{U_{эфф}(\tau,f)}}$$

где: $U_{\min}$ — минимально допустимая полнота для запуска корректных алгоритмов восстановления, а α характеризует, насколько критичен дефицит данных. При этом рост τ и f ведет к увеличению загрузки канала, которую можно условно представить функцией затрат ресурсов $R(\tau,f)$.

Таким образом, оптимизационная постановка сводится к выбору τ и f следующим образом:

$$\min_{\tau,f} R(\tau,f)\Big|U_{эфф}(\tau,f)\geq U_{\min},$$

то есть требуется минимизировать нагрузку на сеть при обеспечении достаточной полноты информации. Рассматриваемое расширение *Management Information Base* (*MIB*) включает новые OID, отражающие заданные τ и f, а также дополнительные типы *Trap*-сообщений. Существенным элементом является адаптивное изменение этих параметров в оперативном режиме при возникновении критических факторов (воз-

[3]Боевое применение подразделений связи, узлов связи соединений, объединений Сухопутных войск. Учебник: Часть 2 / Под ред. О. П. Тевса. – СПб.: ВАС, 2021. – 476 с.

растание помех, колебания температур, перебои электропитания), что позволяет автоматизированно переходить от ограниченного мониторинга к детальному без чрезмерной нагрузки на сеть в нормальных условиях эксплуатации.

Анализ условий эксплуатации и необходимость адаптивного мониторинга

Условия ведения современных операций осложняются не только наличием огневого воздействия противника, но и масштабным радиоэлектронным и информационным противодействием. Использование средств подавления связи может приводить к фрагментации и даже временному исчезновению некоторых каналов [6]. Пропускная способность при этом становится крайне ограниченной, а задержки в передаче данных возрастают. Стандартный SNMP, ориентированный на стабильные каналы, не предусматривает эффективных механизмов адаптации. Например, при попытке использовать подробные MIB-объекты в условиях высокой потери пакетов возрастает вероятность недостоверности данных, и повторные опросы могут существенно ухудшить оперативность процесса сбора информации.

Дополнительная проблема связана с климатическими особенностями регионов, где развертываются узлы связи специального назначения. Экстремальные температурные режимы, сильные порывы ветра и резкие колебания влажности приводят к сбоям в работе ТКО, что требует повышения точности мониторинга их технического состояния. Наряду с этим, нестабильное электроснабжение, вызванное перегрузками на электрогенераторах, приводит к кратковременным отключениям оборудования, что усиливает потребность в оперативном контроле. При этом традиционная реализация *SNMP*, основанная на постоянном высоком уровне детализации и частом опросе, перегружает и без того низкоскоростные каналы связи, что негативно сказывается на своевременности и точности диагностики.

Особую актуальность приобретает требование по обеспечению скрытности обмена данными. При активном функционировании системы мониторинга избыточный трафик может быть обнаружен средствами радиоэлектронной разведки противника [6], что повышает риск идентификации и последующего подавления ключевых каналов связи. Требования безопасности связи диктуют необходимость минимизации служебного трафика в режимах нормальной работы, с переходом в режим повышенного сбора данных лишь при возникновении критических ситуаций. Стандартный *SNMP* не предусматривает механизмов динамического изменения частоты опроса и глубины диагностирования, что ограничивает его применение в условиях, где требуется адаптивное управление информационными потоками. В источниках по системам военного назначения [7, 8] подчеркивается важность внедрения интеллектуальных алгоритмов мониторинга, способных учитывать текущую радиочастотную обстановку и оперативно корректировать политику сбора данных. Таким образом, адаптивный механизм мониторинга является необходимым ответом на ограничения пропускной способности каналов, угрозу перехвата информации, нестабильность энергоснабжения и неблагоприятные климатические условия. В предлагаемом решении модернизация *SNMP* достигается за счет дополнения *MIB* новыми идентификаторами и введения дополнительных *Trap/Inform*-сообщений, что позволяет оператору централизованно регулировать уровень детализации и частоту запросов. Такая архитектурная модификация обеспечивает возможность оперативного переключения между режимами минимального обмена данными в стандартном режиме эксплуатации к режиму детального анализа при возникновении критических событий, что существенно повышает отказоустойчивость системы без избыточной нагрузки на каналы связи.

Модель эффективной полноты информации мониторинга

Разработка адаптивных стратегий невозможна без формализации самого понятия «полнота информации», нужной для диагностики. Одним из подходов к количественной оценке полноты целесообразно считать подход моделирования эффективной полноты информации, в которой вводятся параметры и весовые коэффициенты, показывающие, какой набор данных и с какой точностью необходим пользователю на различных уровнях управления. При этом показателем эффективной полноты $U_{эфф}(\varepsilon,\tau)$ может быть показатель, учитывающий, степень детализации, важной для конкретного уровня управления (ε) и класса информационных требований (τ).

В более общем виде модель эффективной полноты информации может быть записана следующим образом:

$$U_{эфф}(\varepsilon,\tau)=\sum_{i=1}^{m}U_i w_i(\varepsilon,\tau)$$

где:

ε — параметр, характеризующий иерархический уровень пользователя (например, более высокий уровень управления требует более агрегированной, но менее детализированной инфор-

мации);

τ — параметр, отражающий класс информационных требований (набор параметров или профиль данных, необходимых для данного уровня управления);

значения U_i соответствуют базовой полноте i-го класса данных, а $w_i(\varepsilon,\tau)$ — весовые коэффициенты, отражающие значимость данного класса данных для конкретного иерархического уровня и информационного профиля.

Реальная эффективность диагностики зависит не только от количества собираемых данных, но и от того, насколько оперативно они могут быть получены и обработаны. Для учета этой временной компоненты используется поправочный множитель, отражающий чувствительность процесса устранения отказа к отношению $U_{\min} / U_{эфф}(\varepsilon,\tau)$, где $U_{\min}$ — минимально необходимая полнота для запуска корректных алгоритмов диагностики. Исходя из общих идей теории достаточной статистики [6], время диагностики и устранения неисправностей может расти при недостающем объеме данных. Для этой зависимости часто используется рациональная аппроксимация:

$$\Delta T_{диагн} = \frac{1}{1+\alpha\dfrac{U_{\min}}{U_{эфф}(\varepsilon,\tau)}},$$

где α характеризует, насколько критично уменьшение полноты данных относительно необходимого минимума. При $U_{эфф}(\varepsilon,\tau) >> U_{\min}$ значение $\Delta T_{диагн}$ близко к 1, то есть дополнительные задержки в диагностике практически отсутствуют. Если же $U_{эфф}(\varepsilon,\tau)$ близко к $U_{\min}$ или даже меньше, то $\Delta T_{диагн}$ уменьшается, отражая рост временных затрат на уточнение и верификацию ограниченных данных. При этом своевременность и полнота диагностики ТКО напрямую влияют на время восстановления работоспособности узла связи (включая замену неисправных компонентов, перегруппировку маршрутов и т.д.).

Применительно к элементам телекоммуникационных сетей специального назначения, где установка дополнительных датчиков или модулей слежения часто ограничена весовыми, энергетическими и маскировочными требованиями, необходимо найти компромисс между развернутым сбором сведений обо всех потенциальных сбоях и минимально достаточным набором параметров, который обеспечивает заданный уровень готовности и быстрого реагирования. Слишком подробная информация увеличивает трафик, усложняет передачу и анализ данных, но при этом ускоряет поиск неисправностей. Недостаточная информация снижает точность, может задержать принятие решения о ремонте и вызвать дополнительные риски при эксплуатации в боевых условиях. Введение в *SNMP* механизма динамического управления глубиной мониторинга и частотой опроса позволяет приблизиться к оптимальному балансу, когда $U_{эфф}(\varepsilon,\tau)$ превышает $U_{\min}$ ровно в той мере, в которой это необходимо по текущей обстановке, не создавая лишнего трафика при нормальном режиме функционирования телекоммуникационной сети.

Методологические подходы к оптимизации структуры системы мониторинга

Для того чтобы предложенная модель была работоспособной, необходимо сформулировать задачу формирования и выбора оптимального варианта набора мониторинговых параметров (или датчиков) и адаптивной частоты опроса, соответствующей текущим условиям. В литературе по беспроводным сенсорным сетям [9, 10] указывается, что при решении подобных задач применяются подходы, основанные на решении задачи покрытия (*Coverage Problem*) и адаптивной стратегии изменения частоты опроса (*Adaptive Sampling*). Несмотря на то, что данные исследования чаще рассматривают классические *WSN*, изложенные там идеи релевантны для сетей специального назначения, где набор *SNMP*-агентов с соответствующими *OID* фактически выступает в роли аналогов сенсорных узлов.

Задача покрытия нацелена на поиск минимального множества датчиков $\Theta^* \subseteq \Theta$ из доступного полного набора Θ, при котором совокупный вклад в полезную полноту $U_{эфф}(\varepsilon,\tau)$ не меньше $U_{\min}$. При этом учитывается, что у каждого датчика есть собственная «стоимость» в виде объема данных, формируемых при опросе, что влияет на загруженность канала и время обработки. Решение, как правило, строится на «жадных» (*greedy*) алгоритмах: на каждом шаге выбирается датчик, дающий наибольший прирост полезной полноты относительно стоимости, и так далее, пока $U_{эфф}(\varepsilon,\tau)$ не достигнет $U_{\min}$. Такой принцип позволяет сократить избыточный набор датчиков и снизить вероятность перегрузки сети.

Кроме определения необходимой полноты и множества датчиков, важно также определить частоту опроса. В условиях стационарных сетей обычно задают постоянные интервалы опроса, достаточные для стандартной диагностики. Однако в динамической обстановке, когда уровень помех или интенсивность использования канала может резко возрасти, либо появиться сбои в энергоснабжении, требуется адаптивная страте-

гия. Она предполагает увеличение частоты опроса в периоды, когда оборудование находится в зоне риска (перегрев, высокий уровень битовых ошибок, перегрузка канала), и снижение частоты при благоприятной обстановке. Это позволяет, с одной стороны, своевременно выявлять любые опасные тенденции, а с другой — не тратить лишний трафик и вычислительные ресурсы в спокойных режимах. Формализовать вклад отдельных датчиков в общее значение $U_{эфф}(\varepsilon,\tau\{f_j\})$ можно введением частот $\{f_j\}$, учитывающих качество и актуальность данных.

При реализации адаптивного подхода менеджер должен иметь инструменты оперативной смены как состава отслеживаемых параметров, так и частоты их опроса. Здесь в игру вступает расширенный протокол *SNMP*, в котором появятся новые *OID*, отвечающие за глубину детализации (*oidDetailLevel*) и частоту опроса (*oidSamplingFreq*). В формализованном виде итоговую эффективную полноту можно представить следующим образом:

$$U_{эфф}\left(\varepsilon,\tau,\left\{f_j\right\}\right)=\sum_{\theta_j\in\Theta^*}U_i w_i\left(\varepsilon,\tau,\left\{f_j\right\}\right),$$

где U_j — базовая полнота данных от j-го датчика (или параметра), а w_j — весовой коэффициент, зависящий не только от уровня управления и информационного профиля, но и от фактической частоты опроса $\{f_j\}$. Возрастание $\{f_j\}$ позволяет собирать более детализированные данные за единицу времени, но увеличивает нагрузку на канал и может способствовать росту пропускных задержек. Правильно выстроенная оптимизационная задача выбирает такое множество датчиков Θ^* и такие частоты $\{f_j\}$, которые обеспечивают $U_{эфф}(\varepsilon,\tau\{f_j\})\geq U_{min}$ при минимизации нагрузки на сеть, времени сбора информации и риска ее перехвата.

Решение поставленной задачи и результаты исследования

Предлагаемая концепция модернизации *SNMP* реализует гибкое управление глубиной мониторинга и частотой опроса ТКО, что особенно актуально в полевых узлах связи с ограниченным ресурсом пропускной способности каналов связи. Ключевым элементом является дополнение *MIB* новыми OID, такими как *oidDetailLeve*l (управление уровнем детализации) и *oidSamplingFreq* (динамическая настройка частоты опроса). На рисунке 1 демонстрируется базовая архитектура: менеджер (Server) взаимодействует с несколькими *SNMP*-агентами, а также с интеллектуальным блоком *ML*, который анализирует телеметрию (например, показатели помех, состояние питания) и формирует рекомендации по оптимальным значениям новых *OID*.

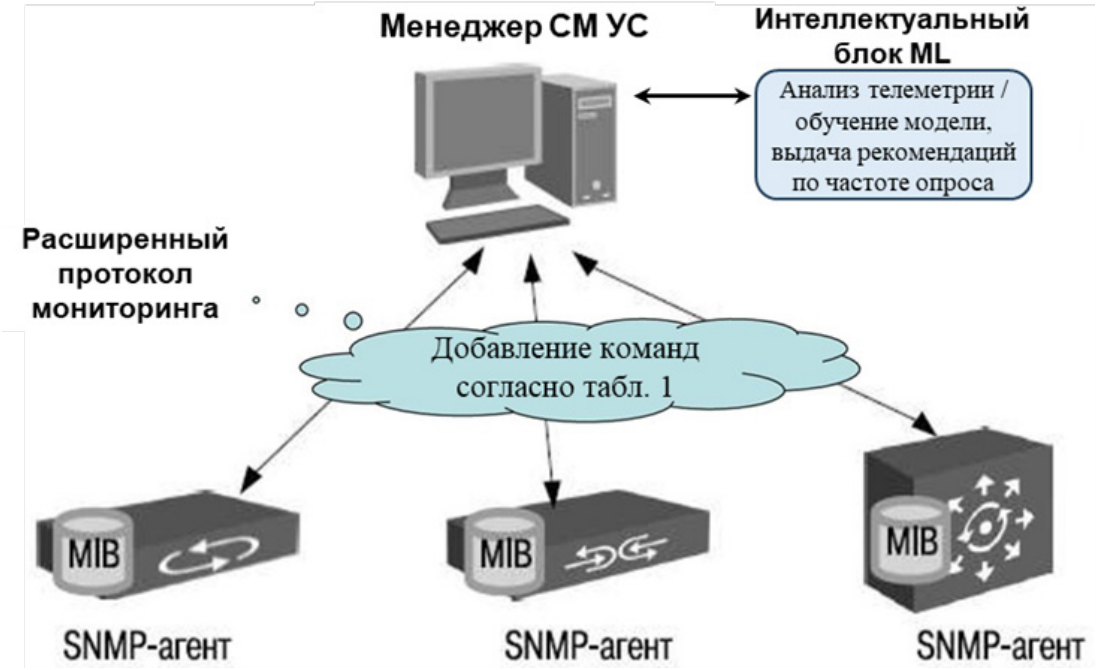

Рис. 1. Предлагаемая система управления мониторингом технического состояния ТКО с использованием модернизированного протокола

В таблице 1 приведены существующие команды (*Get, Set, GetNext*), а также новые команды (*oidDetailLevel, oidSamplingFreq*) для направления *Server → Agent*. Аналогичные изменения затрагивают и направление *Agent → Server*, где наряду с классическими *Trap* и *Inform*-сообщениями появляются дополнительные уведомления (*TrapExcessiveBER, TrapTempWarning*), позволяющие информировать менеджер о критических состояниях с необходимым уровнем детализации. Так, при низком уровне детализации агент может передавать лишь сигнальные уведомления, а при повышенной детализации — отправлять более обширные сведения о причинах сбоев и динамике параметров (включая время фиксации, историю журналов и т. д.).

Таблица 1

Расширение команд «менеджер – агент» в SNMP

Команды менеджера (Server → Agent)	Сообщения агента (Agent → Server)
Существующие: - **Get** – запрос значения (чтение параметра) - **Set** – установка значения параметра - **GetNext** — последовательное чтение следующего объекта MIB	**Существующие:** - **Trap** – аварийное (асинхронное) уведомление без подтверждения от сервера - **Inform** – уведомление с подтверждением от сервера
Новые: - **oidDetailLevel** – настройка уровня детализации параметров - **oidSamplingFreq** – настройка частоты опроса параметров *Фактически это новые OID в MIB для динамического управления глубиной детализации и частотой опроса.*	**Новые:** - Дополнительные Trap/Inform (например, ***TrapExcessiveBER, TrapTempWarning***) – позволяют агенту сообщать более подробную или менее детализированную информацию о состоянии оборудования в зависимости от настроек *Включают расширенный набор полей (OID) для передачи дополнительных сведений.*

Расширенный протокол мониторинга базируется на восьми этапах (рис. 2), которые позволяют систематизировать процесс разработки и внедрения модернизированного протокола мониторинга ТКО на узлах связи специального назначения.

Рис. 2. Алгоритм разработки и внедрения расширенного протокола SNMP

Рассмотрим каждый шаг алгоритма:

1. Определение требований к мониторингу. Изучаются факторы, влияющие на надежность ТКО (риск деструктивных воздействий). На основе этого задается минимально необходимая полнота данных U_{min} и временные ограничения сбора измерительной информации и диагностики объектов мониторинга.

2. Анализ существующей *MIB*. Выполняется оценка текущих объектов (OID), поддерживаемых в узлах связи. Определяется набор недостающих переменных (например, показатели температуры, *BER*, состояние блоков питания), а также необходимость динамического управления их опросом. Формализация эффективности мониторинга может быть выражена суммой значимостей данных U_j с учетом весовых коэффициентов w_j.

3. Формирование новых *OID* и *Trap*-сообщений. Разрабатываются oidDetailLevel и *oidSamplingFreq*, а также дополнительные *Trap*-сигналы (*TrapExcessiveBER, TrapTempWarning*) для уведомления о перегревах, всплесках битовых ошибок и др. Критерием полноты выступает $U_{эфф} \ge U_{min}$, что гарантирует достаточный набор данных для диагностики.

4. Внесение изменений в агенты. *SNMP*-агенты дополняются реализацией новых *OID*: поддерживаются механизмы «*Set*» для *oidDetailLevel* и *oidSamplingFreq*, а также обработчики новых *Trap*-сообщений (*TrapHandlers*). В программном

обеспечении агентов учитываются формулы расчета нагрузки на канал ($\Lambda_j = W_j \times f_j$), чтобы избегать перегрузок.

5. Внесение изменений на менеджере. Управляющая станция (менеджер) получает возможность изменять параметры глубины детализации и частоты опроса по протоколу *SNMP* (команды из таблицы 1). Дополнительно интегрируется блок ML, который, анализируя получаемые *Trap/Inform*-уведомления, способен на лету корректировать политику опроса. Благодаря этому в периоды спокойной обстановки детальность снижается (не перегружая канал), а при обнаружении признаков опасных сбоев (например, берущихся из *TrapExcessiveBER*) повышается частота и глубина мониторинга.

6. Тестирование и оценка нагрузки. На опытных стендах моделируются различные сценарии (резкие изменения внешней температуры, скачки напряжения, помехи). Проверяется, что система корректно переключается между низкой и высокой детальностью, а итоговая нагрузка на канал удовлетворяет неравенству $T_{сб} \leq T_{сб}^{доп}$.

7. Внедрение в опытную эксплуатацию и корректировка. Расширенная система развертывается в реальной (или приближенной к реальной) среде. На основании полученных данных корректируются отдельные пороги, значения α в выражении (4) и параметры обучения блока *ML*, обеспечивая оптимальную реакцию на сбои.

8. Вывод результатов (готовое решение).

Завершающий этап предполагает формирование полностью работоспособного варианта «менеджер–агент» с новыми *OID* и *Trap*-сообщениями. Такая модернизация *SNMP* обеспечивает адаптивное управление мониторингом, сокращает $\Delta T_{диагн}$, улучшает скрытность за счет снижения избыточного трафика[4] в нормальном режиме и позволяет в случае угроз быстро активировать режим детального сбора данных.

В условиях боевых действий и прочих критических ситуаций возможность вариативного контроля глубины диагностики и частоты опроса является ключом к эффективной эксплуатации узлов связи. Благодаря интеллектуальному блоку ML и расширенным *Trap*-сообщениям система способна мгновенно реагировать на нештатные события, сводя к минимуму риск отказа ТКО и обеспечивая непрерывность управления. Такой подход во многом определяет результативность операции и пригоден как для стационарных сетей с повышенными требованиями к надежности, так и для высокодинамичных полевых условий.

Предлагаемый подход к модернизации *SNMP*, может позволить динамически управлять глубиной и частотой мониторинга ТКО в полевых условиях, демонстрирует при этом высокую работоспособность и эффективность. Реализованная архитектура (расширенная *MIB*, новые *OID*, дополнительные *Trap*-сообщения и интеллектуальный блок) способны удовлетворить поставленным требованиям, обеспечивая достаточную полноту данных при минимальном риске перегрузки сети.

Практический пример расчёта трафика мониторинга в условиях ограниченной пропускной способности канала

Рассмотрим пример расчёта нагрузки на спутниковый канал пропускной способностью 2 Мбит/с (2048 Кбит/с), отражающий типичные условия эксплуатации сетей специального назначения при ограниченном ресурсе спутниковой связи в ходе ведения, например, наступательной операции. Данные каналы, как правило, одновременно обслуживают телеметрический трафик, каналы управления, а также голосовую и прикладную информацию, что существенно повышает требования к оптимизации объёма служебной нагрузки. Даже сравнительно небольшое по абсолютной величине количество мониторинговых сообщений способно вызвать избыточную загрузку, особенно при наличии криптографических накладных расходов и высокой задержки (*RTT*) характерной для спутниковых систем связи.

Приведённые ниже расчёты наглядно демонстрируют, каким образом предложенный подход к адаптивному управлению глубиной детализации и частотой опроса может повысить эффективность использования канала и сократить риск деградации критически важного трафика.

Исходные данные:

Полоса пропускания канала спутниковой связи:

2 Мбит/с ≈ 250 Кбайт/с.

При круглосуточной работе суммарная суточная пропускная способность без учёта накладных расходов протоколов и потерь пакетов может достигать:

250 Кбайт/с × 3600 × 24 ≈ 21,6 Гбайт в сутки.

Конфигурация сети:

Наблюдаемая телекоммуникационная система содержит 20 объектов мониторинга (маршрутизаторы, коммутаторы, мультиплексоры и т. п.), каждый с 50 ключевыми параметрами (*OID*) для мониторинга.

В классическом подходе (стандартный

[4]Нефедов, В. И. Общая теория связи: учебник для вузов / В. И. Нефедов, А. С. Сигов; под редакцией В. И. Нефедова. — Москва: Издательство Юрайт, 2024. — 592 с. — (Высшее образование). — ISBN 978-5-534-19215-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/556153 (дата обращения: 03.02.2025).

SNMP) все параметры опрашиваются с равными интервалами, без учёта текущих условий.

Размер SNMP-сообщений:

Один запрос (Get) на 1 OID — около 200–400 байт (включая *IP/UDP/SNMP* заголовки и полезную нагрузку).

Типичный ответ (*Response*) — 300–500 байт.

При использовании *SNMPv3* с аутентификацией и шифрованием объём может вырасти ещё на 20–30%.

Временная задержка (latency) для геостационарного спутника: 500–600 мс в одну сторону (RTT ≈ 1–1,2 с). В условиях ведения операции задержки могут быть ещё интенсивнее, а потери пакетов — выше.

Сценарий 1. Стандартный *SNMP* (без адаптивных механизмов).

Частота опроса — опрос всех 50 OID на каждом из 20 объектов мониторинга каждые 5 секунд.

Объём данных на один полный цикл:

Запрос на 50 OID (20 устройств) = 50 × 20 = =1000 запросов, каждый запрос ~ 300 байт => => 1000 × 300 = 300000 байт или ≈ 300 Кбайт только на запросы.

Ответы по 400 байт => 1000 × 400 = = 400000 байт или ≈ 400 Кбайт.

Итого на один 5-секундный цикл приходится ~700 Кбайт.

Нагрузка в секунду: 700 Кбайт / 5 с = = 140 Кбайт/с ≈ 1,12Мбит/с.

Процент загрузки 2-Мбит/с канала: около 56%.

В течение суток: (700 Кбайт / 5 с) × 17280 пятисекундных интервалов в сутках ≈ 12,1 Гбайт (Без учёта возможных повторных запросов при потерях пакетов и накладных расходов криптографической защиты).

Как показывают представленные расчёты, при использовании стандартной схемы интенсивного опроса в сравнительно крупной сети для одного низкоскоростного канала (20 объектов мониторинга с 50 контролируемыми параметрами и короткими интервалами опроса) формируемый служебный трафик может существенным образом исчерпать доступную полосу пропускания, оставляя недостаточно ресурсов для приоритетной передачи оперативной информации предназначения канала.

Сценарий 2. Расширенный *SNMP* с динамической детализацией и частотой опроса.

В этом варианте используется механизм адаптивной перестройки:

1. Базовый режим «*Base (LOW)*».

Частота опроса — один раз в 5 минут (300 секунд).

Опрашиваются 10 необходимых из 50 возможных *OID* на каждом объекте мониторинга, наиболее критичные (например, состояние питания, ошибка канала, суммарный уровень *BER*).

Таким образом, за цикл (300 секунд) при 20 объектах мониторинга опрашивается 20 × 10 = = 200 *OID*. Если в среднем 300 байт на запрос и 400 байт на ответ, то можно получить: 200 × (300 + + 400) = 200 × 700 = 140,000 байт ≈ 140 Кбайт за 300 секунд.

Среднее в секунду — 140 Кбайт / 300 с ≈ ≈ 0,47 Кбайт/с ≈ 3,76Кбит/с. Это составляет ≈ ≈ 0,19% от пропускной способности канала в 2 Мбит/с.

Подобный режим действует при отсутствии признаков аварий или критических событий. Трафик в сутки — 140 Кбайт × 86400 с ≈ 40,3 Мбайт.

2. Углублённый режим «*HIGH*».

Активируется при поступлении тревожных *Trap*-сообщений (*TrapExcessiveBER, TrapTempWarning*) или при превышении пороговых значений по критическим *OID*.

В этом случае менеджер может установить частоту опроса 1 раз в 10 секунд для 20–25 необходимых *OID* (более детальный набор). Размер *SNMP*-сообщений также может возрасти за счёт передачи расширенной диагностической информации (например, 400–500 байт на запрос, 500– 600 байт на ответ).

Предполагается, что авариный режим длится 2 часа в сутки. За этот период опрашивается ≈ 25 *OID* на 20 устройствах каждые 10 секунд — 20 × 25 = 500 *OID* за цикл.

Если суммарный объём запроса и ответа на один *OID* составляет ~1000 байт, то за 10 с формируется около 500 Кбайт данных (или 50 Кбай т/с = 400 кбит/с). Это соответствует примерно 20 % загрузки 2 Мбит/с канала в течение данного интервала.

За 2 часа (7200 с) генерируется ≈ ≈ (500 Кбайт / 10с) × 720 = 360000 Кбайт = = 360 Мбайт.

Итоговая суточная нагрузка:

- 22 часа в базовом режиме (*LOW*) — 22 × × (40,3 / 24) ≈ 36,9 Мбайт.
- 2 часа в режиме (*HIGH*) — 360 Мбайт.
- Итого ≈ 397 Мбайт за сутки, что существенно ниже 12,1 Гбайт, получающихся при классическом сценарии (рис. 3). Кроме того, высокая интенсивность («*HIGH*») действует только в течение ограниченного двухчасового интервала, позволяя большую часть времени сохранять минимальную нагрузку.

Проведённые расчёты показывают, что в

случае классической реализации *SNMP* с фиксированной частотой и максимальным набором *OID* даже относительно небольшое увеличение числа объектов может привести к значительному росту нагрузки на канал (достигая 50–60 % пропускной способности при 2 Мбит/с). Вместе с тем, предлагаемый адаптивный механизм позволяет оптимизировать объём мониторингового трафика в периоды нормальной эксплуатации и автоматически повышать детальность опроса при обнаружении потенциальных отказов. Это высвобождает резерв пропускной способности канала для передачи оперативных сообщений и критически важных команд в телекоммуникационных системах специального назначения. Приведённый пример демонстрирует, что динамическое управление глубиной детализации и частотой опроса снижает совокупную нагрузку без ущерба для эффективности диагностики при возникновении сбоев, аномалий и отказов.

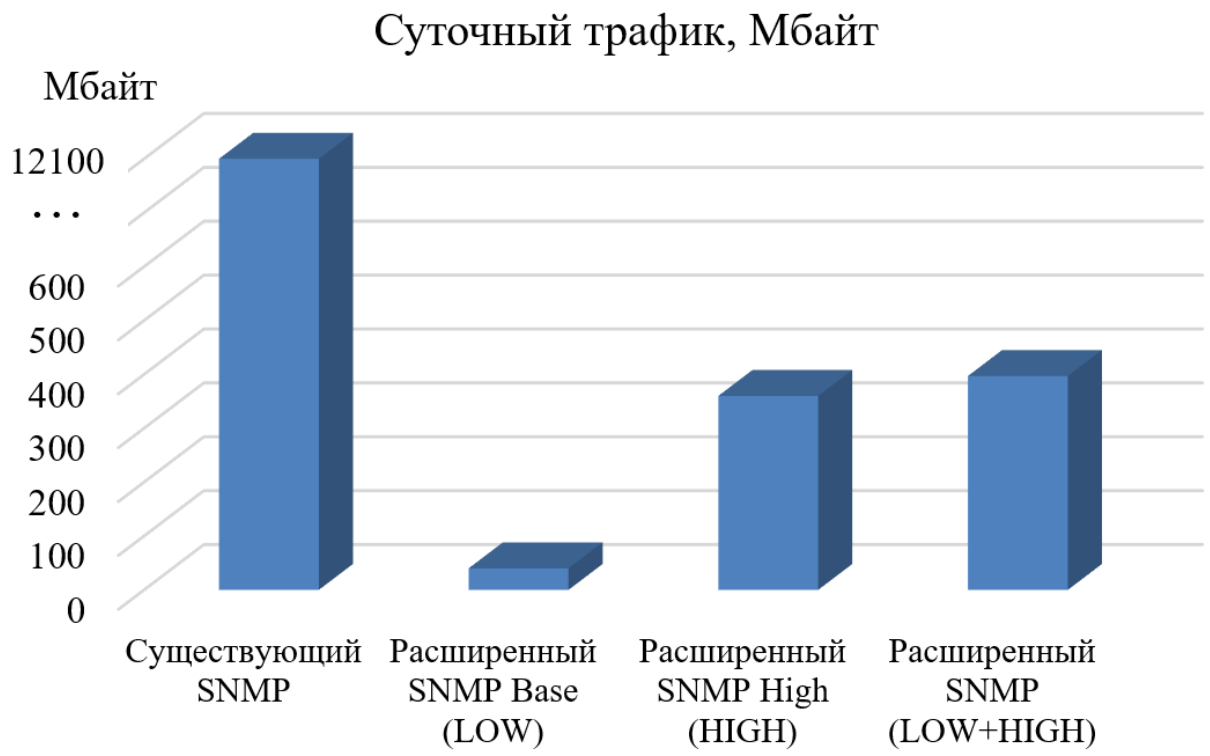

Рис. 3. Сравнение суточного трафика мониторинга (2 Мбит/с)

Выводы

Подход к модернизации протокола *SNMP* ориентирован на решение задач обеспечения надежного, скрытного и оперативного мониторинга узлов связи специального назначения, действующих в условиях ограниченной полосы пропускания, переменной помеховой нагрузки и риска целенаправленного подавления связи. В отличие от классической схемы *SNMP*, где механизмы мониторинга статичны, предложенное расширение *MIB* и новые типы команд (*oidDetailLevel и oidSamplingFreq*) дают возможность динамически управлять глубиной детализации и частотой опроса данных. Формируемая архитектура «менеджер–агент» становится более гибкой: агент способен переходить от упрощенного к детализированному режиму в режиме реального времени, а менеджер может централизованно задавать эти переключения в зависимости от конкретной обстановки. Дополнительные типы *Trap/Inform*-сообщений позволяют пересылать более полные сведения о сбоях, когда это необходимо, не перегружая при этом канал постоянным транзитом большого объема диагностических данных.

Адаптивность достигается благодаря использованию модели эффективной полноты информации, в которой учитывается не только объем собираемых параметров, но и их критичность для конкретного уровня управления. Расширенный SNMP, тем самым, способен поддерживать оптимальный баланс между избыточностью трафика в спокойное время и достаточной полнотой данных для быстрой диагностики в моменты критических сбоев. На уровне формальных методов

это реализуется путем решения задач покрытия, снижающих избыточность набора датчиков, и адаптивного выбора частот опроса, сокращающего излишнюю загрузку канала и ускоряющего анализ в важные периоды. Результатом становится уменьшение $\Delta T_{\text{диагн}}$, приводящее к более быстрому восстановлению сети при отказах и снижению общей уязвимости системы управления.

Предложенная концепция реализации расширенного *SNMP* соответствует растущим требованиям к безопасности и эффективности военных систем связи. Экономия ресурсов в спокойном режиме и возможность оперативного наращивания полноты мониторинга при выявленных угрозах существенно повышают жизнестойкость и скрытность сети. Испытания такой системы в реальных условиях ведения боевых действий должны подтвердить ее способность гибко реагировать на комплекс внешних факторов, включая возможные сбои в питании, климатические воздействия и враждебные радиоэлектронные атаки. В перспективе данный подход может быть интегрирован не только в военные сети, но и в другие типы систем, где присутствуют повышенные требования к адаптивности, скорости реакции и экономии ресурса канала передачи данных. Все это делает предложенное решение актуальным и востребованным в условиях современных операций, требующих надежного функционирования телекоммуникационной инфраструктуры при одновременно ограниченных и подверженных противодействию ресурсах.

Литература

1. Блинова, О. В. Проектирование сетей связи быстрого развертывания с использованием программного приложения анализа конфигурации сети / О. В. Блинова, С. В. Васьковкий, Я. В. Рыков // Управление большими системами: сборник трудов. – 2021. – № 90. – С. 121–138. – DOI: 10.25728/ubs.2021.90.6
2. Боговик, А. В. Проблемы организации мониторинга телекоммуникационного оборудования узлов связи пунктов управления оперативного объединения и пути их решения / А. В. Боговик, Д. М. Сафиулов // Известия Тульского государственного университета. Технические науки. – 2024. – № 5. – С. 196–198. – DOI: 10.24412/2071-6168-2024-5-196-197
3. Мансуров, Т. А. Мониторинг устройств по технологии SNMP, находящихся в сети / Т. А. Мансуров, В. Е. Марлей, С. Ю. Соклакова // Информационные системы и технологии. – 2021. – № 5(127). – С. 91–95. – EDN AYELWE
4. Боговик, А. В. Анализ существующих систем мониторинга технического состояния телекоммуникационного оборудования сетей связи / А. В. Боговик, Д. М. Сафиулов // Известия Тульского государственного университета. Технические науки. – 2023. – № 5. – С. 112–117. – DOI: 10.24412/2071-6168-2023-5-112-113
5. Чикин, А. В. Достаточные статистики в задаче мониторинга спутниковых каналов TDMA / А. В. Чикин // Труды Научно-исследовательского института радио. – 2009. – № 3. – С. 108–119. – EDN KYNLND
6. Перунов, Ю. М. Радиоэлектронная борьба в информационных каналах: монография / Ю. М. Перунов, А. И. Куприянов. Москва — Вологда: Инфра-Инженерия, 2021. 452 с. - ISBN 978-5-9729-0718-2.
7. Боговик, А. В. Методологический подход к формированию архитектуры системы мониторинга технического состояния техники связи / А. В. Боговик, Д. М. Сафиулов // Известия Тульского государственного университета. Технические науки. – 2024. – № 2. – С. 176–182. – DOI: 10.24412/2071-6168-2024-2-176-177
8. Боговик, А. В. Предложения по повышению эффективности технического диагностирования типовых элементов замены телекоммуникационного оборудования / А. В. Боговик, А. А. Бурлаков, Д. М. Сафиулов // Проблемы технического обеспечения войск в современных условиях: Материалы VIII межвузовской научно-практической конференции, Санкт-Петербург, 14 апреля 2023 года. – Санкт-Петербург: Военная академия связи, 2023. – С. 60–65. – EDN HBUNRJ
9. Эрзин А. И. Модели и методы оптимизации беспроводных сенсорных сетей // – Труды Международной конференции по информационным наукам и технологиям связи. – 2018. – Т. 1, № 1. – С. 1–5. – EDN HLLHRU
10. Мальцева, Н. С. Анализ способов построения беспроводных сенсорных сетей / Н. С. Мальцева, А. Д. Зубова, И. Н. Марышева // Инженерно-строительный вестник Прикаспия. – 2018. – № 2(24). – С. 31–36. – EDN ZLWNMU

PROPOSALS FOR MODERNIZATION OF THE PROTOCOL FOR MONITORING TELECOMMUNICATIONS EQUIPMENT OF A SPECIAL-PURPOSE COMMUNICATION CENTER

Bogovik A.V.[1], Safiulov D.M[.2]

Keywords: *remote diagnostics, adaptive data collection, hierarchical structures of MIB (Management Information Base), field conditions, electronic countermeasures, channel reliability, intelligent configuration, flexible detailing*

Abstract

The purpose of *the article is to analyze the existing methods of collecting and processing data on the state of telecommunications equipment of special-purpose communication networks and to develop proposals for the implementation of remote adaptive diagnostics, taking into account the features of field conditions and high requirements for secrecy.*

The research methods *consist in the use of comparative analysis mechanisms in the process of managing network devices, formalized models of information completeness and algorithms of the required coverage to optimize the structure of the set of sensors used. The methodological basis was the work on improving the stability of sensor networks in the face of limited resources, modeling and expert evaluation, which made it possible to identify key performance indicators proposed approach.*

Results of *the study. In the course of the work, the problems arising during the operation of communication nodes in conditions of limited channel bandwidth and high risk of electronic countermeasures are analyzed. It is shown that the standard mechanism of remote monitoring, which provides for constant detail and uniform polling frequency, in a combat situation leads to an excessive amount of service traffic and can unmask important elements of the infrastructure. The strategy allows you to dynamically change the depth of diagnostics and data acquisition intervals, avoiding overloading network resources. This is achieved by adding new identifiers and trap messages to the MIB parameter library, which are activated only when threats or deviations from normal operating modes are detected. The proposed approach significantly reduces the time to detect malfunctions, increases the speed of their elimination and reduces the risk of losing critical information, which is extremely important for field military systems and associated communication centers. In addition, adaptive polling rate algorithms are considered in detail, which reduce the load during periods of stable operation and immediately increase the sensitivity of monitoring in the event of abnormal situations. This flexibility provides both effective diagnostics and the necessary level of stealth.*

The scientific novelty of the *work lies in the proposal of formal models based on the effective completeness of data and coverage tasks, which make it possible to quantitatively substantiate the choice of monitoring depth and survey frequency. The introduction of new identifiers and messages in the MIB opens up additional opportunities for intelligent reconfiguration of monitoring agents, taking into account the dynamics of the situation and limited channel resources.*

References

1. Blinova, O. V. Proektirovanie setej svjazi bystrogo razvertyvanija s ispol'zovaniem programmnogo prilozhenija analiza konfiguracii seti / O. V. Blinova, S. V. Vas'kovkij, Ja. V. Rykov // Upravlenie bol'shimi sistemami: sbornik trudov. – 2021. – № 90. – S. 121–138. – DOI: 10.25728/ubs.2021.90.6
2. Bogovik, A. V. Problemy organizacii monitoringa telekommunikacionnogo oborudovanija uzlov svjazi punktov upravlenija operativnogo ob#edinenija i puti ih reshenija / A. V. Bogovik, D. M. Safiulov // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. – 2024. – № 5. – S. 196–198. – DOI: 10.24412/2071-6168-2024-5-196-197
3. Mansurov, T. A. Monitoring ustrojstv po tehnologii SNMP, nahodjashhihsja v seti / T. A. Mansurov, V. E. Marlej, S. Ju. Soklakova // Informacionnye sistemy i tehnologii. – 2021. – № 5(127). – S. 91–95. – EDN AYELWE
4. Bogovik, A. V. Analiz sushhestvujushhih sistem monitoringa tehnicheskogo sostojanija telekommunikacionnogo oborudovanija setej svjazi / A. V. Bogovik, D. M. Safiulov // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. – 2023. – № 5. – S. 112–117. – DOI: 10.24412/2071-6168-2023-5-112-113
5. Chikin, A. V. Dostatochnye statistiki v zadache monitoringa sputnikovyh kanalov TDMA / A. V. Chikin // Trudy Nauchno-issledovatel'skogo instituta radio. – 2009. – № 3. – S. 108–119. – EDN: KYNLND
6. Perunov, Ju. M. Radiojelektronnaja bor'ba v informacionnyh kanalah: monografija / Ju. M. Perunov, A. I. Kuprijanov. Moskva – Vologda: Infra-Inzhenerija. 2021. 452 s. ISBN 978-5-9729-0718-2.

[1]Alexander V. Bogovik, Ph.D., Professor, Professor of the Department of the Military Academy of Communications, St. Petersburg, Russia. E-mail: bogovikav@mail.ru

[2]Davlet M. Safiulov, Adjunct of the Military Academy of Communications, St. Petersburg, Russia. E mail: davletzas@mail.ru

7. Bogovik, A. V. Metodologicheskij podhod k formirovaniju arhitektury sistemy monitoringa tehnicheskogo sostojanija tehniki svjazi / A. V. Bogovik, D. M. Safiulov // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. – 2024. – № 2. – S. 176–182. – DOI: 10.24412/2071-6168-2024-2-176-177
8. Bogovik, A. V. Predlozhenija po povysheniju jeffektivnosti tehnicheskogo diagnostirovanija tipovyh jelementov zameny telekommunikacionnogo oborudovanija / A. V. Bogovik, A. A. Burlakov, D. M. Safiulov // Problemy tehnicheskogo obespechenija vojsk v sovremennyh uslovijah: Materialy VIII mezhvuzovskoj nauchno-prakticheskoj konferencii, Sankt-Peterburg, 14 aprelja 2023 goda. – Sankt-Peterburg: Voennaja akademija svjazi, 2023. – S. 60–65. – EDN: HBUNRJ
9. Jerzin A. I. Modeli i metody optimizacii besprovodnyh sensornyh setej // – Trudy Mezhdunarodnoj konferencii po informacionnym naukam i tehnologijam svjazi. – 2018. – T. 1, № 1. – S. 1–5. – EDN: HLLHRU
10. Mal'ceva, N. S. Analiz sposobov postroenija besprovodnyh sensornyh setej / N. S. Mal'ceva, A. D. Zubova, I. N. Marysheva // Inzhenerno-stroitel'nyj vestnik Prikaspija. – 2018. – № 2(24). – S. 31–36. – EDN: ZLWNMU