УДК 004.72:616-036(575.2)

УНИВЕРСАЛЬНАЯ ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА ДЛЯ МОНИТОРИНГА ЭПИДЕМИОЛОГИЧЕСКОЙ ОБСТАНОВКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

С.В. Корякин

Рассматриваются вопросы построения универсальной телекоммуникационной системы (ТКС) с использованием универсальной среды проектирования автоматизированных систем с элементами встроенных систем реального времени. Разрабатываемая ТКС поддерживает полный цикл автономных автоматизированных систем, обеспечивается возможность их скоростного имитационного моделирования и отработка алгоритмов. Приведено описание разработанной универсальной телекоммуникационной системы для мониторинга параметров окружающей среды Кыргызской Республики.

Ключевые слова: модель; этапы проектирования; среда проектирования; системы реального времени (СРВ); автоматизированная система защищенного исполнения.

КЫРГЫЗ РЕСПУБЛИКАСЫНДАГЫ ЭПИДЕМИОЛОГИЯЛЫК АБАЛГА МОНИТОРИНГ ЖҮРГҮЗҮҮ ҮЧҮН УНИВЕРСАЛДУУ ТЕЛЕКОММУНИКАЦИЯЛЫК СИСТЕМА

С.В. Корякин

Бул макалада реалдуу убакыт системаларынын элементтери бар автоматташтырылган системаларды долбоорлоонун универсалдуу чөйрөсүн пайдалануу менен универсалдуу телекоммуникациялык системаларды түзүү маселеси каралган. Иштелип чыккан телекоммуникациялык системалар автономдук автоматташтырылган системалардын толук циклин кодойт, аларды тездетилген имитациялык моделдөө мүмкүндүгү жана алгоритмдерди иштеп чыгуу камсыздалат. Кыргыз Республикасынын курчап турган чөйрөсүнүн параметрлерине мониторинг жүргүзүү үчүн иштелип чыккан универсалдуу телекоммуникациялык системанын сүрөттөлүшү берилген.

Түйүндүү сөздөр: модель; долбоорлоо этаптары; долбоорлоо чөйрөсү; реалдуу убакыт системасы; корголгон аткаруудагы автоматташтырылган система.

UNIVERSAL TELECOMMUNICATION SYSTEM FOR MONITORING THE EPIDEMIOLOGICAL SITUATION IN THE KYRGYZ REPUBLIC

S.V. Koryakin

The article discusses the issues of building a software and hardware core (complex) of a universal automated system using embedded real-time systems. The complex supports the full development cycle, providing the possibility of high-speed simulation of the created systems and development of algorithms. The description of the developed universal telecommunication system for monitoring environmental parameters of the Kyrgyz Republic is given.

Keywords: Model; design stages; design environment; real-time systems (RTS); automated secure execution system.

Задачей универсальной телекоммуникационной системы (ТКС) является автоматизированное моделирование систем управления процессами, а также информационная поддержка мер по своевременному прогнозированию, выявлению, предупреждению угроз и кризисных ситуаций, а также при ликвидации последствий реализации угроз.

Разработанная система мониторинга параметров окружающей среды далее (СМПОС) позволяет получать сведения со всех наиболее опасных районов Кыргызской Республики во время различных стихийных бедствий (эпидемии, землетрясения, паводки, сели, оползни и др.). Структурная схема СМПОС представлена на рисунке 1.

СМПОС обладает разветвленной сетью, состоящей из центров коммутаций, расположенных в местах с повышенной опасностью эпидемиологических вспышек и стихийных бедствий по всей территории Кыргызской Республики. Поскольку СМПОС должна обладать высокой степенью надежности и универсальностью при модернизации при ее создании используются современные технологии передачи и хранения информации, так называемые облачные технологии и принцип кластеризации элементов системы. В качестве систем передачи информации планируется использовать многоуровневую систему каналов передачи данных как традиционных и широко используемых во всем мире проводных и беспроводных технологий передачи данных (радио, радиорелейные, спутниковые, оптические), так и инновационных, к примеру, передача информации при помощи PLC технологий.

Региональные сети ИИС (СМПОС). Прогнозирование на основе информации параметров окружающей среды, полученных в горных и отдаленных селах Кыргызской Республики, осложняется отсутствием центров диагностики и наблюдений за различными вредоносными и опасными параметрами. Именно поэтому существует большая потребность в сверхкраткосрочном прогнозе опасных эпидемиологических и иных явлений для отдаленных населенных пунктов и других объектов экономики с высокой достоверностью. Эта потребность диктуется высокой необходимостью принятия оперативных мер по защите населения от вспышек пандемии (вплоть до эвакуации). Решить эту проблему становится возможным при использовании всех имеющихся ведомственных и региональных ресурсов. В этом случае всю полноту ответственности за обеспечение безопасности жизнедеятельности населения непосредственно несут руководители муниципальных и региональных органов власти, которые нуждаются в оперативном и достоверном получении информации о ЧС, либо об угрозе ЧС, локализации места ЧС и ее масштабов. Создание таких систем позволит принять своевременные и адекватные меры по защите населения.

Именно поэтому автор предлагает спроектировать СМПОС по принципу кластеризации. Ядро системы предлагается расположить в г. Бишкек, как в административном центре страны, остальные центры коммутации – в областных и региональных центрах, а также непосредственно в местах съема параметров окружающей среды. Систему предполагается построить таким образом, чтобы в случае отказа ядрового центра коммутации вместо него управление системой смог принимать любой другой центр коммутации независимо от географического месторасположения, на время, пока ядровой центр коммутации не будет восстановлен. Таким образом, надежность системы будет повышена до максимально возможного уровня и сможет сохранять работоспособность в режиме работы «24/7».

Обработка данных мониторинг ПС. Обработка данных будет обеспечиваться территориальным центром мониторинга и прогнозирования чрезвычайных ситуаций природного и техногенного характера (ТЦМП) МЧС Кыргызской Республики. После развертывания всех элементов СМПОС, специалистами ТЦМП должна быть проведена нивелировка всех экологических постов, определены уровни допустимых и предельных параметров для каждого поста, все показания сенсоров датчиков необходимо будет привести к принятой системе высот, что позволит объединить в единую систему мониторинга и прогнозирования все экологические посты, находящиеся на территории Кыргызской Республики [1].

Наряду со специалистами ТЦМП, наблюдение за активностью параметров окружающей среды непрерывно смогут вести оперативные дежурные единых дежурно-диспетчерских служб муниципальных образований, а при достижении уровня эпидемиологической ситуации отметок допустимых или

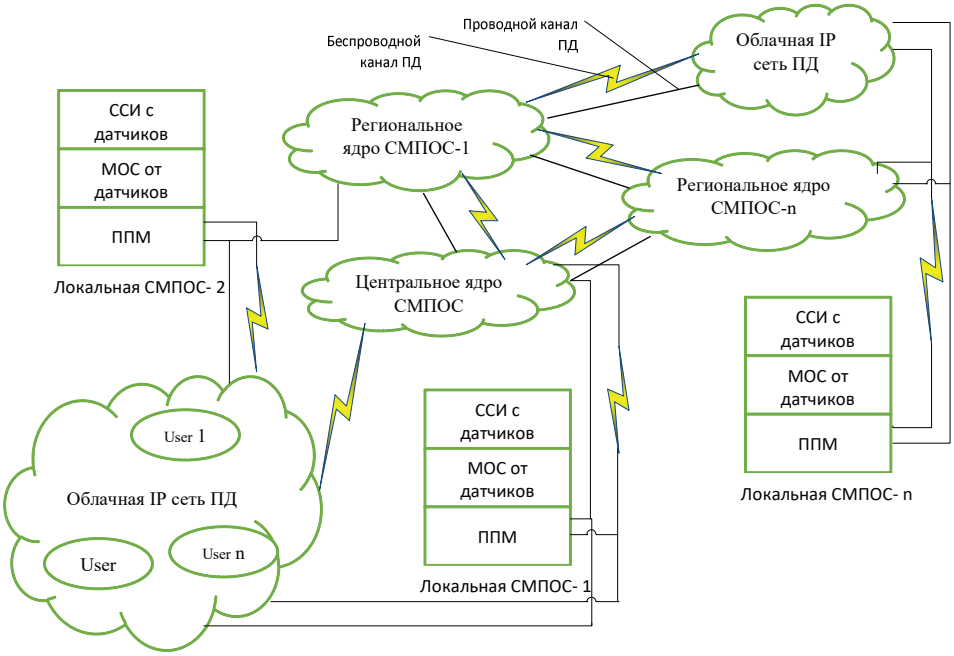

Рисунок 1 – Структурная схема СМПОС: ССИ – система съема информации с датчиков; МОС – модуль обработки сигналов с датчиков, ППМ – приемо-передающий модуль

предельных параметров СМПОС будет производиться автоматическое голосовое оповещение должностных лиц МЧС КР и сил реагирования.

Такой подход обеспечит возможность спасательным службам выдвинуться оперативно в зону предполагаемого ЧС, что при скоротечности развития пандемии и других стихийных бедствий позволит минимизировать ущерб и самое главное – сохранить человеческие жизни.

Таким образом, учитывая современные тенденции развития телекоммуникационных систем, на передний план выходит постоянно растущая и динамически меняющаяся сложность архитектуры распределенных телекоммуникационных систем в целом, а также предлагаемой универсальной телекоммуникационной системы (ТКС) для определения параметров окружающей среды, увеличения количества уязвимостей ТКС и потенциальных ошибок в их функционировании. В составе универсальной ТКС должны быть мощные интеллектуальные системы и модули защиты для противодействия информационным угрозам. Именно поэтому при проектировании и построении ТКС на передний план выходят две основные задачи, которые необходимо решать:

1. Обеспечение надежности распределенной ТКС и функционирующих в ней прикладных информационных систем, гарантированно устойчивых к вредоносным воздействиям и компьютерным атакам, что, как правило, сопряжено с существенными затратами как времени, так и материальных ресурсов.
2. Обеспечение работоспособности распределенной ТКС и расчет наработки на отказ.

Кроме того, существует известная обратная зависимость между удобством пользования системой и её защищённостью – чем совершеннее системы защиты, тем сложнее пользоваться основным функционалом информационной системы.

К настоящему времени опубликован ряд работ, раскрывающих различные подходы к моделированию информационных атак и анализу защищенности, из них можно выделить: метод анализа изменения состояний; причинно-следственную модель атак [1]; описательные модели сети и злоумышленников [2]; структурированное описание на базе деревьев; использование и создание графов атак для анализа уязвимостей; объектно-ориентированное дискретное событийное моделирование и др. Тем не

менее, методы обнаружения воздействий на ТКС и защиты от них в современных распределенных ТКС недостаточно проработаны в части формальной модели, так называемой атаки, для которой достаточно сложно строго оценить такие параметры, как вычислительная сложность, корректность, завершимость и т. д.

Поэтому возрастает необходимость разработки как адекватных моделей распределенных ТКС, так и информационных атак, исследования их влияния на распределенную ТКС с целью совершенствования системы и обеспечения информационной безопасности [3].

Расчет основных показателей надежности, защищенности отказоустойчивости проектируемой системы СМПОС будем производить средствами и инструментами Универсальной среды проектирования автоматизированных систем защищенного исполнения [4], которая имеет встроенные программно-аппаратные средства проектирования структуры и расчетов основных показателей и компонентов ТКС. Ниже рассмотрим основные теоретические аспекты расчета основных показателей ТКС, которые в своей работе использует УСП АСЗИ.

Целевое назначение и классификация методов расчета. В данном случае используются адаптированные расчеты надежности, применяемые для определения количественных надежностей автоматизированных систем.

Существует большое разнообразие расчетов надежности в зависимости от их цели. На рисунке 2 показаны основные виды расчетов надежности.

Выбор того или иного вида расчета надежности определяется заданием на расчет надежности. На основании задания и последующего изучения работы устройства (по его техническому описанию) составляется алгоритм расчета надежности, т. е. последовательность этапов расчета и расчетные формулы.

Последовательность расчета систем показана на рисунке 3. Рассмотрим основные ее этапы.

Прежде всего, следует четко сформулировать задание на расчет надежности. В нем должны быть указаны:

1) назначение системы, ее состав и основные сведения о функционировании;

2) показатели надежности и признаки отказов, целевое назначение расчетов;

3) условия, в которых работает (или будет работать) система;

4) требования к точности и достоверности расчетов, к полноте учета действующих факторов [5].

На основании изучения задания делается вывод о характере предстоящих расчетов. В случае расчета функциональной надежности осуществляется переход к этапам 4-5-7, в случае расчета элементов (аппаратурной надежности) – к этапам 3-6-7.

Под структурной схемой надежности понимается наглядное представление (графическое или в виде логических выражений) условий, при которых работает или не работает исследуемый объект (система, устройство, технический комплекс и т. д.). Типовые структурные схемы показаны на рисунке 4 [5].

Простейшей формой структурной схемы надежности является параллельно-последовательная структура. На ней параллельно соединяются элементы, совместный отказ которых приводит к отказу. В последовательную цепочку соединяются такие элементы, отказ любого из которых приводит к отказу объекта.

На рисунке 4 представлен вариант параллельно-последовательной структуры. По этой структуре можно заключить, что расчет надежности в рассматриваемом случае сводится к расчету отдельных участков схемы, состоящих из параллельно и последовательно соединенных элементов.

Расчет трафика АСМПОС производился согласно основным алгоритмам, используемым для расчета трафика, которые хранятся в библиотеке универсальной среды проектирования УСП АСЗИ. В основе расчета лежат вероятностные характеристики потока данных, которые генерируются различными сетевыми устройствами.

При использовании данной методики в нашем случае необходимо иметь информацию:

- *о приблизительной структуре сети,*
- *о количестве абонентов в каждом узле сети,*
- *о распределении абонентов по различным классам обслуживания,*

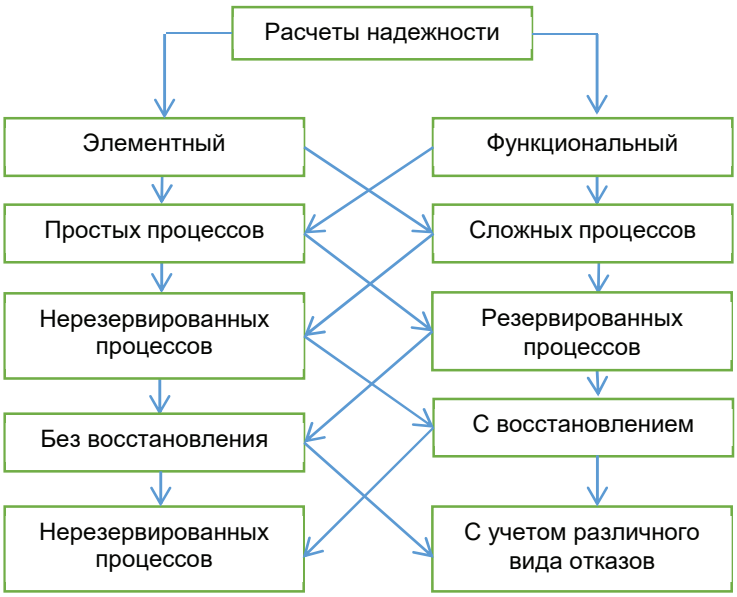

Рисунок 2 – Классификация расчетов надежности

Рисунок 3 – Алгоритм расчета надежности

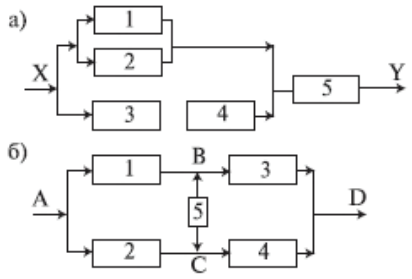

Рисунок 4 – Типовые структуры расчета надежности

- *о перечне сетевых услуг,*
- *о характеристике услуг.*

В библиотеках УСПАСЗИ представлены два основных способа расчета внутренней нагрузки и исходящего трафика:

1. Первый способ состоит в задании коэффициентов, которые показывают долю трафика в каждом направлении:

k1 – во внутреннюю сеть,

k2 – в соседние узлы,

k3 – в другие сети.

При этом имеет место соотношение:

k1+k2+k3 = 1.

2. На каждом этапе анализа сетевой услуги определяют, какие услуги являются внутренними, какие связаны с соседними узлами, а какие – с внешними сетями [6].

Расчет трафика для локальной сети СМПОС. Локальная сеть СМПОС – это сеть, характеризующаяся высокой скоростью, большой пропускной способностью, низким уровнем ошибок передачи, эффективным, быстродействующим механизмом управления обменом и в которой имеется ограниченное, точно определенное число компьютеров, подключаемых к сети.

Помимо своего прямого назначения, локальная сеть для СМПОС должна поддерживать такие услуги, как датчики охраны, устройства контроля замков, IP-телефонию, системы видеонаблюдения, обычную телефонную связь. Функционирование СМПОС как производственного помещения предъявляет к сети дополнительные требования: удобство, высокую работоспособность, гибкость и надежность. Поэтому правильный подбор оборудования, основанный на расчете информационных потоков (трафика), является основой хорошей локальной сети.

Расчет трафика для такой сети – это расчет (прогноз) возможного объема информационных потоков устройств сети и подбор линий связи, обеспечивающих как внешнее, так и внутреннее их взаимодействие. При этом телефонный трафик рассматривается отдельно от компьютерного трафика сети [7].

Предложенный способ расчета является теоретическим и описывает алгоритм расчета универсальной среды проектирования АСЗИ, при помощи которой будет производиться проектирование ТКС – системы для измерения параметров окружающей среды.

Облачные библиотеки, входящие в состав универсальной среды проектирования, позволят смоделировать основные параметры проектируемой системы – учет как входящего, так и исходящего трафика отдельно взятых пользователей. Основываясь на данных мониторинга сети, можно уточнить прогноз, скорректировать объем передаваемой информации и оптимально подобрать параметры сети [8, 9].

Основные направления развития системы АСМПОС:

1. Увеличение времени реагирования на угрозы эпидемиологического характера до 3–4 часов за счет дооснащения системы сенсорами и датчиками, расположенными по всей территории Кыргызской Республики.

2. Прогноз вспышек эпидемий за счет установки датчиков анализа вирусов на существующие экологические посты по всей страны.
3. Увеличение достоверности тревожной информации;
4. Обеспечение обмена эпидемиологической информацией с МЧС.
5. Создание специализированного АРМ дежурного эпидемиолога.
6. Мониторинг эпидемиологической обстановки.

Для создания системы мониторинга, пригодной по своим параметрам для непрерывного наблюдения естественных объектов и инженерных сооружений, планируется использовать массив сенсоров-датчиков, определяющих уровень вредоносных частиц и вирусов.

При мониторинге общий рукав с массивом сенсоров-датчиков размещается в специализированных экологических постах, предназначенных для мониторинга эпидемиологической ситуации.

Выводы. Предложен новый подход для решения всех основных проблем, возникающих во время построения, а также при адаптации после внедрения и при дальнейшей модернизации спроектированных моделей, автоматизированных для мониторинга параметров окружающей среды, работающих в режиме реального времени. Описан новый алгоритм работы АСМПОС и ее функционал, предложен вариант специализированной системы сенсоров-датчиков для определения уровня опасных микроорганизмов, веществ и вирусов.

Сформулирована классификация и дано определение модулей, выполняющих функцию работы процессов АСМПОС. Предложена новая структура модуля, выполняющего функцию имитации работы процессов АСЗИ, в виде основного компонента системы для построения имитационных моделей АСМПОС. Определены и классифицированы элементы АСМПОС. Приведена классификация основных системных модулей и ключевых позиций компонентов системы, а также дано математическое описание расчета основных показателей системы.

Таким образом, предложенная модель АСМПОС позволит сократить временные затраты на согласование времени и способа построения различных систем мониторинга, повысить надежность, универсальность, а также снизить число ошибок при планировании и проектировании АСЗИ.

Литература

1. *Курзыкина А.В.* Проблемы внедрения автоматизированной информационной системы / А.В. Курзыкина // Молодой ученый. 2017. № 4. С. 124–167. URL: https://moluch.ru/archive/138/38806/ (дата обращения: 16.03.2020).
2. *Гомах U.M.*L. Проектирование систем реального времени, параллельных и распределенных приложений / U.M.L. Гомах; пер. с англ. М.: ДМК Пресс, 2011. 704 с. (Сер. Объектно-ориентированные технологии в программировании). С. 115–174.
3. *Брякин И.В.* Проектирование автоматизированных систем защищенного исполнения / И.В. Брякин. Бишкек, 2017. С. 1–24.
4. *Леонтьев В.П.* Персональный компьютер / В.П. Леонтьев. М.: ОЛМА Медиа групп, 2008. 800 с.
5. *Yuill J.* Intrusion-detection for incidentresponse, using a military battlefield-intelligence process / J. Yuill, F., J. Wu. Settle, F. Gong // Computer Networks. 2000. No. 34.
6. *Cohen F.* Simulating Cyber Attacks, Defenses, and Consequences / F. Cohen // IEEE Symposium on Security and Privacy. Berkeley, CA, 1999.
7. *Dawkins J.* Modeling network attacks: Extending the attack tree paradigm / J. Dawkins, C. Campbell, J. Hale // Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection. Johns Hopkins University, 2002.
8. *Chi S.-D.* Network security modeling and cyber at-tack simulation methodology / S.-D. Chi, J.S. Park, K.-C. Jung, J.-S. Lee // Lecture Notes in Computer Science. Springer-Verlag. V. 2119, 2001.
9. *Шипачев В.С.* Высшая математика. Полный курс: учебник для бакалавров / В.С. Шипачев; под ред. А.Н. Тихомирова. 4-е изд. М.: Юрайт, 2012. 607 с.