ПУТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ГОСУДАРСТВЕННОГО И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ

д.т.н., проф. Петров А.Б., заместитель проректора по учебной работе, заведующий кафедрой корпоративных информационных систем МГТУ МИРЭА
к.т.н., доц. Андрианова Е.Г., доцент кафедры корпоративных информационных систем МГТУ МИРЭА, Сычева А.И., главный научный сотрудник ФГУП «НИИ «Восход»», Багров С.В., ассистент кафедры корпоративных информационных систем МГТУ МИРЭА.

Краткая аннотация: *рассматривается новый подход к обеспечению безопасности функционирования распределённых информационных систем государственного и муниципального управления на основе анализа информационных процессов.*

Ключевые слова: *безопасность функционирования, информационные системы, информационные технологии, системы с предсказуемым поведением, открытые системы.*

Введение

Развитие информационной инфраструктуры государственного, регионального и муниципального управления связано с формированием сложной, многосвязной среды на основе распределенных информационных систем (РИС), для которых помимо традиционных аспектов надежности, важными становятся аспекты живучести и аспекты устойчивости, связанные с обеспечением продолжения выполнения функций в условиях отказа части системы. В настоящее время эффективная и безопасная работа РИС определяется потенциальной опасностью возможных последствий неадекватного поведения элементов РИС по отношению к объекту управления, человеку, окружающей среде. Соответственно, появляется новая характеристика РИС – безопасность функционирования [1-3].

Повышение безопасности функционирования РИС требует заблаговременного проведения комплекса мероприятий, направленных на максимально возможное уменьшение риска возникновения чрезвы-чайных ситуаций, а также на сохранение здоровья людей, снижение размеров ущерба окружающей при-родной среде и материальных потерь в случае их возникновения, а также проведения экспертизы пред-полагаемых для реализации проектов и решений, которые могут быть источниками чрезвычайных ситуаций, в целях проверки и выявления степени их соответствия установленным нормам, стандартам и правилам [2].

Пути решения

Существует много аспектов анализа РИС для обеспечения безопасности функционирования [4-6]:

- с точки зрения аппаратной реализации;
- с учетом операционной и системной среды;
- как комплексную аппаратно-программную платформу;
- используя систему оценки рисков;
- анализируя информационные потоки;
- анализируя внутреннюю структуру программной среды реализации информационной системы;
- анализируя алгоритм программной среды реализации ин-формационной системы;
- анализируя функциональное представление информационной системы;
- анализируя архитектурное функциональное представление информационной системы;
- анализируя процессы взаимосвязи двух и более информационных систем,

- анализируя конкретную информационную технологию либо набор базовых информационных технологий,

- анализируя процессы взаимодействия информационных технологий,

- оценивая экспертным путем возможные последствия.

Общая задача повышения безопасности функционирования РИС тесно связана с применением методов создания систем с предсказуемым поведением, включающим метод комплексного анализа (МКА), метод приближенного анализа (МПА), метод анализа на основе тестирования устройств и систем (МАТС) [1, 2].

Для обеспечения практического применения этих методов возможны различные уровни рассмотрения, в том числе важным и информативным является рассмотрение на уровне информационных процессов, когда анализируется правильность реализации всех заложенных в информационную систему информационных процессов [5-6].

В начальный момент мы формируем описание информационной системы исходя из набора элементов системы и набора связей между ними с установлением перечня информационных потоков, соответствующих каждой из связей. Определяется набор, накладываемых на элементы системы, связи между ними, а также на общие характеристики и качество функционирования системы в целом. Строится орграф системы, в котором вершинами будут элементы, а дугами – связи между ними.

После этого, мы рассматриваем интегральную характеристику, определяющую процедуру, качество и соответствие ожидаемым результатам при обработке информации для элемента системы, определяем интервал возможных значений этой характеристики.

Деля общий интервал возможных значений на подинтервалы и формируя перечень возможных состояний элемента получаем через значение функции принадлежности [2-3] состояние рассматриваемого элемента одному из возможных состояний. Проводя операции пересечения и объединения на основе подходов нечеткой логики, мы получаем традиционный [3-4] набор результатов анализа.

Осуществляя последовательный обход по орграфу всех путей и корректируя текущее описание элемента с учетом влияния смежных с ним элементов, с последующей дефаззификацией этих результатов, мы получаем перечень элементов информационной системы, потенциально являющихся источниками опасностей, оценку гарантированной работоспособности системы в целом, а также возможные последствия неадекватного поведения элементов на результаты функционирования системы в целом.

Заключение

Рассматриваемые методы дают значимые результаты только с одной точки рассмотрения проблемы обеспечения безопасности функционирования в условиях неадекватного поведения элементов информационной системы. Вводя другие аспекты рассмотрения, можно получить иные, уточняющие результаты. Комплексный анализ получаемых при таком рассмотрении результатов, дополненный традиционными оценками надежности, а также оценками рисков дает сводную картину по выявлению «слабых» элементов в системе, оценке источников потенциальных опасностей и прогнозированию возможных последствий.

Литература

1. Петров А.Б. О повышении безопасности функционирования сложных систем. - Информатизация и системы управления в промышленности. №4, 2004 – с.37-39

2. Петров А.Б. О повышении безопасности устройств и систем. - "Надежность" №4 (15) 2005 г. - с. 3-7.

3. Петров А.Б. Применение технологии открытых систем для создания систем с предсказуемым поведением - Информационная техника и вычислительные системы, №3, 2003 – с.61-63.

4. Петров А.Б., Сычева А.И. Вопросы обеспечения безопасности функционирования сложных распределенных систем государственного назначения. - 12 научно-практическая конференция «Современные информационные технологии в управлении и образовании». - М., ФГУП НИИ «Восход», 18 апреля 2013 г. Сб. трудов. Т.1 – с.7-11

5. Петров А.Б., Сычева А.И. Применение методов функциональной стандартизации для обеспечения безопасности функционирования сложных распределенных информационных систем государственного назначения. - Сб. трудов IV Международной конференции «ИТ-стандарт 2013» М., 22-23 октября 2013 года – с.84-87.

6. Петров А.Б., Сычева А.И. О безопасности функционирования сложных информационных систем в информационной среде. - 13 научно-практическая конференция «Современные информационные технологии в управлении и образовании». -М., ФГУП НИИ «Восход», 17 апреля 2014 г. Сб. трудов. Т.1 – с.11-16.