ВВЕДЕНИЕ

Роль и место системной инженерии на современном этапе развития сложных технических систем трудно переоценить. До недавнего времени наука развивалась по пути совершенствования отдельных элементов, процессов, операций, технологий в сложных технических системах. Были достигнуты определенные результаты в различных предметных областях. Полученные результаты не в полной мере определяют системный эффект (эффективность функционирования) сложной технической системы. Одна из основных причин отсутствия системных результатов — это использование традиционных методов исследования, направленных на получение «точечных» оценок. Однако известные методы исследования не позволяют оценить сложные технические системы в комплексе. Исследуются в отдельности функционал, структура, организация системы, а человеческий фактор не рассматривается. Кроме того, результаты исследований сложных технических систем с использованием известных методов в динамических условиях показывают недостаточную результативность и высокую погрешность. В работе предлагаются подходы (способы, приемы, методы), позволяющие оценить (с использованием «интервальных» оценок) сложные технические системы в динамических условиях с достаточно низкой погрешностью, выявить системные противоречия и определить пути их устранения.

Книга состоит из трех глав.

Первая глава посвящена рассмотрению основных элементов системной инженерии — определений и терминов, подходов и принципов применения, а также предложен вариант применения системной инженерии при синтезе систем обеспечения информационной безопасности.

Вторая глава содержит описание основных методов и приемов, применяемых при решении изобретательских задач, а также примеры использования методов вепольного, диверсионного, функционально-стоимостного анализа и схем обусловленности

взаимодействий при решении задач синтеза систем обеспечения информационной безопасности.

В третьей главе предложены подходы и даны примеры формулирования квалификационных признаков диссертационных исследований на основе применения подходов системной инженерии и теории решения изобретательских задач в области информационной безопасности.

Глава 1

Основы теории системной инженерии в области информационной безопасности

1.1. Общие положения системной инженерии

1.1.1. Этапы становления системной инженерии

XX век, особенно его вторую половину, можно охарактеризовать как время развития сложных разнородных технических систем (например, развитие пилотируемой космонавтики, ядерная энергетика и ее практическое применение в атомоходе «Ленин» и др.). Объединение разнородных систем позволило в значительной мере расширить возможности эксплуатируемых систем, однако потребовало от разработчиков новых специфических знаний по управлению сложными проектами.

Термин «системная инженерия» (*Systems Engineering*) стал впервые использоваться в корпорации Bell Labs в 40-х годах XX века.

Один из основоположников теории систем Людвиг фон Берталанфи выделил системную инженерию в качестве прикладной составляющей теории (рис. 1.1).

Системная инженерия — научное планирование, проектирование, оценка и конструирование систем человек-машина.

Исследование операций — научное управление существующими системами людей, машин, материалов и др.

Инженерная психология — анализ приспособления систем (прежде всего машинных систем) для достижения максимума эффективности при минимуме денежных и иных затрат.

Одним из первых системных инженеров в СССР по праву можно считать С.П. Королёва. Его заслуга заключается не только в разработке непосредственно ракеты «Восток 1», но и в создании всей необходимой сопутствующей инфраструктуры: стартового стола, систем связи и слежения, системы подготовки космонавтов, систем снабжения и многих других (причем зна-

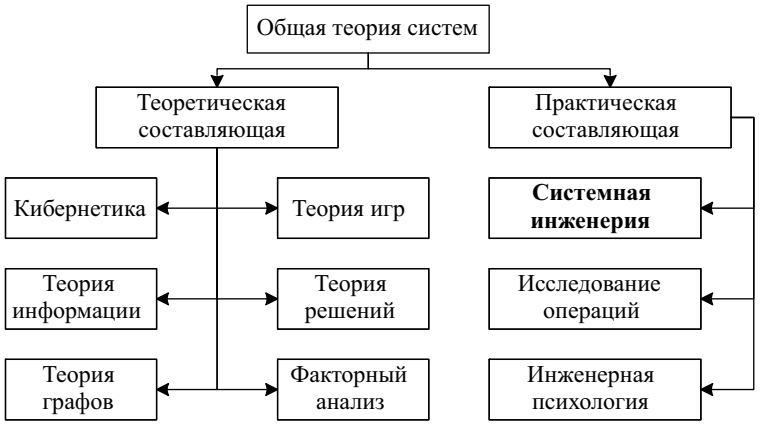

Рис. 1.1. Структура общей теории систем (Л. фон Берталанфи)

чительная часть систем создавалась либо впервые, либо существенно видоизменялась). Помимо синтеза С.П. Королёв решал задачи эксплуатации и, в частности, вопросы технического обслуживания (ремонтнопригодности), эргономики, безопасности и утилизации.

Перечисленные задачи стремились рассматривать в теории управления, кибернетики, системном анализе и др. В указанный временной период зарождается системная инженерия, одной из первых работ в данной области можно считать монографию Г.Х. Гуда и Р.Э. Макола «Системотехника. Введение в проектирование больших систем» (Harry H. Good, Robert E. Machol. Systems Engineering. An Introduction to the Design of Large-Scale Systems, 1957). Авторы рассматривали системную инженерию как инструмент проектирования высокоавтоматизированных сложных технических систем (СТС), описали признаки систем большого масштаба. Также сформулированы проблемы технического и организационно-управленческого характера. В СССР эта книга была переведена под названием «Системотехника» (автор названия — профессор Ф.Е. Темников), и в последующем «системотехника» стала названием научного направления. Однако из-за двойного трактования системотехника со временем в качестве объекта изучения стала рассматривать автоматизированные или автоматические СТС, что превратило ее в прикладную отрасль знаний.

Согласно А. Холлу (1962 г.) системная инженерия направлена на исследование потребностей, и в ее в основе лежит использо-

вание передовых экономических теорий, учет потребностей рынка и возможности изменения этих потребностей.

Развитие системной инженерии как самостоятельной теории потребовало развитие терминологического базиса. Так, в качестве основных инструментов познания и систем и деятельности в системной инженерии применяется термин «подход»:

- системный подход (1971 г., Калифорнийский технологический институт, Ч. Черчмен, Р. Говард, Р. Макол, Р. Майлс, С. Рамо и др.);
- интеграционный подход (1976 г., В. Чейз и И. Уимор);
- подход жизненного цикла (1981 г., Б. Бланчард и В. Фабрицкий);
- управленческий подход (1992 г., А. Сэйдж).

Вопросы синтеза системы систем в СССР рассматривались в рамках теории систем и системного анализа. Одним из значимых событий для развития системного анализа послужило создание семинара «Системный анализ в проектировании и управлении» (Ф.Е. Темников, Ю.И. Черняк, В.Н. Волкова, 1973 г.) при Всесоюзном научно-техническом обществе радиотехники, электроники и связи. К ведущим научным школам в предметной области можно отнести школы: С.А. Валуева (Московский экономико-статистический институт), В.Н. Волковой (Ленинградский политехнический институт), Е.П. Голубкова (Московский институт народного хозяйства им. Плеханова), А.И. Костогрызова (Академия наук РФ), Л.Т. Кузина (Московский инженерно-физический институт), Л.А. Растригина (Академия наук Латвийской ССР), Ю.И. Черняка (Центральный экономико-математический институт), Ф.Е. Темникова (Московский энергетический институт) и др.

Особое место в истории системного анализа, кибернетики и системной инженерии занимает «Московский логический кружок» (Б.А. Грушин, А.А. Зиновьев, Г.П. Щедровицкий и др.), впоследствии преобразованный в «Московский методологический кружок», сформулировавший системо-мыследеятельностную методологию (СМД-методология). Дальнейшие исследования в области СМД-методологии позволили сформировать теории деятельности и мышления. Эти теории во многом опередили время и в силу идеологических причин широкого развития не получили.

В силу ряда особенностей развития науки и идеологии в СССР ряд научных течений в прямой постановке не получили

развития (кибернетика, генетика, системная инженерия и др.), однако схожие задачи решались в смежных теориях.

Развитие систем, усложнение разрабатываемых проектов, а также интеграция производств ведущих технологически развитых стран мира в конце 80-х годов XX века обозначили потребность в создании общих стандартов и требований. Устраняя указанную потребность, в начале 90-х годов XX века был создан Международный совет по системной инженерии (International Council on Systems Engineering, INCOSE). В настоящее время в INCOSE функционирует 30 рабочих групп (управление требованиями, управление рисками, архитектура систем, технологии жизненного цикла, верификация и валидация, стандарты и др.) и 50 отделений, действующих по всему миру. Отделение INCOSE в России существует с 2009 г.

В настоящее время системная инженерия активно развивается как в России, так и в мире в целом. Одним из основных издателей литературы по системной инженерии является «Wiley», публикующая серию книг «Systems Engineering & Management», а также журнал «Systems Engineering».

Учитывая прикладной характер, системная инженерия развивает не только теоретический базис, но и активно участвует в формировании нормативной базы. Так, в настоящий момент разработано более 100 документов в области системной инженерии: официальные международные стандарты (JTC1 ISO/IEC); государственные стандарты; профессиональные стандарты и стандарты консорциумов (IEEE, EIA, ECSS, SAE).

Также следует отметить, что системные инженеры активно используют и развивают теорию решения изобретательских задач, например В.К. Батоврин (кафедра «Системная инженерия», Института кибернетики РТУ МИРЭА) и др.

1.1.2. Термины и определения, применяемые в системной инженерии

В системной инженерии, как и в ряде других теорий, существует свой специфический терминологический аппарат, который не применяется в других теориях или имеет иное толкование. Далее представлены базовые определения, в качестве основы авторы использовали группу ГОСТ 2502n «Системная и программная инженерия» [1–3] и ряд других документов и работ в предметной области [4–7].

Системная инженерия — наука о создании крупных комплексных систем, которые соответствуют определенному набору экономических и технических требований.

Системная инженерия — междисциплинарная область технических наук, сосредоточенная на проблемах создания эффективных, комплексных систем.

Системная инженерия — междисциплинарный подход, определяющий полный набор технических и управленческих усилий, необходимых для преобразования совокупности потребностей клиента, ожиданий и ограничений в решении и для поддержки этих решений на протяжении их жизни.

Актор — лицо, выполняющее какое-либо действие с проектом или его частью (этапом). Актором выступают исполнители и инициаторы («заказчик» — стейкхолдер) проекта.

Стейкхолдер — заинтересованное лицо (человек или организация), имеющее определеннный интерес к системе, в том числе к ее функционированию или конструкции, назначению, продукту, какими-либо характеристикам.

Интересы стейкхолдера — набор (совокупность) требований, предъявляемых к системе.

Система — это то, что может быть выделено из окружения, разделено на имеющие связи элементы (конструкцию) и имеет какое-то назначение (функцию) для внешнего окружения. Система обязательно имеет стейкхолдеров.

Границы системы — совокупность связей между элементами системы и внешней средой.

Архитектура системы — структура компонентов, их взаимоотношений, принципов и руководств, направляющих их проектирование с учетом эволюции во времени, связь между нуждами анализа и целью проекта, функциональный анализ и первое описание структуры системы. Архитектура системы может отражаться набором различных инструментов — схем, таблиц, структур, для наиболее полного выражения набора требуемых свойств. Архитектура системы включает: физические характеристики (структура); функции (поведение); параметры (производительность); технологию; стоимость; риски; ограничения; границы системы; интерфейсы системы (внутренние, внешние).

Функциональные связи — каждый элемент выполняет определенные виды работ в рамках единого процесса.

Информационные связи — элементы обмениваются информацией.

Внешние связи — отдельные элементы взаимодействуют с внешними системами, причем их взаимодействие также может быть как информационным, так и функциональным.

Функциональная система предназначена для предоставления функциональных возможностей в заданных условиях (условиях эксплуатации) в интересах удовлетворения потребностей пользователей и иных заинтересованных сторон.

Система обеспечения — система, которая служит дополнением к функциональной системе на протяжении ее жизненного цикла, но не обязательно вносит непосредственный вклад в ее функционирование.

Система систем — набор или упорядоченная совокупность систем, возникающая в результате комплексирования независимых и пригодных к работе систем в более крупную систему, обладающую новыми возможностями.

Виртуальная система систем — система, не имеющая центрального пункта управления, а также единой согласованной цели.

Коллаборативная система систем — система, в которой для достижения согласованных общих целей отдельные системы взаимодействуют без центрального органа управления.

Общепризнанная система систем — система, имеющая осознанные цели, назначенного руководителя и выделенные ресурсы, однако у составляющих ее систем могут быть независимые цели, ресурсы, подходы к разработке и обеспечению функционирования.

Целевая система систем — система, создаваемая для достижения конкретных целей, централизованно управляемая на протяжении всего срока службы для выполнения как известных, так и новых задач.

Назначение процесса — атрибут процесса, характеризующий главную выгоду для стейкхолдеров от выполнения процесса.

Описание процесса — набор фактов о процессе.

Концепция эксплуатации — документ, описывающий характеристики системы с точки зрения пользователя.

Конструкционное описание системы — представление системы в виде взаимосвязанных элементов, из которых состоит система, а также протекающих процессов в них.

Функциональное описание системы — описание, характеризующее назначение системы для ее окружения, и (или) взаимодействие системы как целого и ее окружения.

Опорное описание — описание системы (в том числе процесса), включающие название системы, ее функцию — назначение и перечисление конструкционных элементов (в случае процесса — практик или процессов).

Принципиальное описание процессов — описание реализации протоколов (алгоритмов взаимодействия) между акторами с точки зрения перемещения между ними предметов, данных и управления.

Подход — способ создания, интерпретации и использования в качестве норм описаний системы и правил его применения, используемый для формирования описаний систем и установления деятельностных (процессных) норм. Подход включает: набор стейкхолдеров и их интересов к системе; методы рассмотрения и описания систем и правила их применения, включающие предметную (тематическую) онтологию метода и нотации для графического или текстового представления соответствующих предметной онтологии метода фактов о системе.

Метод описаний — совокупность способов исследования, предназначенная для порождения тематической группы описаний. Методов описаний обязательно несколько, никакая система не может быть надлежащим образом описана одним методом — ибо никогда один метод описаний не сможет охватить все интересы всех стейкхолдеров.

Методика — конкретизация метода, осуществляемая путем указания условий его использования и его инструментария.

Онтология — набор концептов (объектов) и отношений между ними. Онтологии в системной инженерии используются для интеграции различных описаний разрабатываемой системы и оценки адекватности методов описаний интересам стейкхолдеров.

Нотация — совокупность графических (включая буквенно-цифровое) изображений концептов и отношений для какой-то онтологии и правила использования этих изображений для описания мира в терминах концептов и отношений этой онтологии.

Информационная модель системы — набор фактов о системе, используемый для получения информации без непосредственного контакта с системой (*информационная модель* используется только в датацентрическом описании системы в виде совокупности элементов данных, из которых по потребности собираются документы-выписки для удовлетворения интересов).

Информационная модель жизненного цикла — набор фактов о жизненном цикле системы. Информационная модель жизненного цикла подразумевает использование какого-то компьютерного средства моделирования (описания) процессов, из которого составляются отдельные документы-отчеты по потребности. Наличие общей базы данных (фактов) о модели жизненного цикла гарантирует, что различные документы-отчеты не содержат противоречий и описывают одни и те же объекты (процессы, акторов и т. д.) с разных точек зрения (т. е. по разным методикам, описания по которым отражают разные интересы стейкхолдеров).

Жизненный цикл — смена состояний системы (эволюция системы) в период времени от замысла до прекращения ее существования.

Описание жизненного цикла — совокупность описаний процессов, выделяемых в рамках жизненного цикла системы.

Стадия (*жизненного цикла*) — часть жизненного цикла, характеризующаяся относительной стабильностью состояния системы в ходе ее эволюции. Стадии отделены друг от друга *контрольными точками* (точками принятия решений).

Процессы жизненного цикла — это те процессы, которые акторы выполняют над системой и которые меняют состояние системы, заставляя ее эволюционировать в ходе ее жизненного цикла.

Управление жизненным циклом — описание процессов жизненного цикла (а часто и название самой группы процессов жизненного цикла, описанных с использованием такого подхода).

Эволюция системы — то, что происходит с системой во время ее жизненного цикла как итог работы различных акторов (итог выполнения процессов) над системой по реконструкции и продлению срока службы.

Практика — способ группирования работ (практик). Процесс состоит из практик, а практики — из работ.

Специальные свойства системы — это аспект системы, характеризующий удовлетворение специальных интересов ряда стейкхолдеров (например, надежность, ремонтопригодность, безопасность).

Показатели эффективности — показатели успеха практической деятельности, которые непосредственно связаны с достижением показателей назначения, принятых для определенных

условий эксплуатации, т. е. насколько хорошо решение позволяет достичь намеченной цели.

Показатели функционирования — физические или функциональные признаки, имеющие отношение к функционированию системы и пригодные к измерению или оценке в установленных условиях испытаний и (или) функционирования.

Технические показатели — показатели элементов системы, необходимые для определения того, насколько система или элементы удовлетворяют или могут удовлетворять техническим требованиям и целям.

Показатели выполнения проекта — показатели для обнаружения отклонений от планов или технических показателей производства с целью принятия решений в отношении будущей работы или технических вариантов.

Показатели выполнения процесса в организации — измеримые характеристики, показывающие степень, в которой отслеживаются процессы жизненного цикла системы.

1.1.3. Концептуальные направления развития системной инженерии

Помимо терминологического базиса, системная инженерия изменила концептуальные подходы синтеза СТС. Далее указаны основные отличия системной инженерии от «традиционных» [8–10]:

Переход от редукционистского к системному подходу.

Редукционистский подход — выделение отдельных черт исследуемого или проектируемого объекта без обсуждения принципов, по которым эти отдельные черты были выделены.

Системный подход — задает назначение и функции системы и элементов, входящих в нее; определяет границы, отделяющие систему и элементы, входящие от внешней среды; описывает связи между элементами и внешней средой, а также стейкхолдеров, их интересы.

Переход от структурного к процессному подходу. Рассмотрение системы не как статичного объекта, а как динамически изменяющегося, изучение законов эволюции системы на всех этапах жизненного цикла и применение этих знаний для повышения эффективности системы в ходе ее применения по назначению.

Переход от одной группы описаний ко множественности групп описаний. Формирование концепции эксплуатации, состоящей:

- из введения (определение цели, задач, требований и характеристик системы);
- описания эксплуатации системы и особенностей операционной архитектуры;
- описания движущих сил, ограничений применения;
- описания эксплуатационных сценариев;
- реализации выбранной концепции и ее обоснование;
- предлагаемой эксплуатационной архитектуры системы;
- влияния организационной структуры и бизнес-процессов;
- оценки рисков и технологической готовности производства;
- процессов разработки, обслуживания и вывода системы из эксплуатации.

Разрабатываемая система представляется в виде *опорного, конструкционного, функциональьного* и *принципиалььного* описаний.

Переход от рабочего проектирования (конструирования, дизайна) к обязательному предварительному архитектурному. Архитектура описывает основные подсистемы и их взаимодействие в языке, свободном от деталей реализации. Одной архитектуре может соответствовать множество разных реализаций. Архитектурный подход, с одной стороны, сокращает количество возможных вариантов построения системы, с другой стороны, не ограничивает возможности реализации системы, основанной на подгонке системы под имеющуюся элементную базу.

Переход от непосредственной реализации к моделецентричной реализации. Моделецентричный подход позволяет реализовать различные граничные условия функционирования системы без разрушения создаваемой системы, что позволяет уменьшить затраты и время, необходимые на выявление закономерностей поведения системы при изменении различных воздействий (внешних и внутренних). Также применение моделей позволяет оценить эффективность предлагаемых синтезированных вариантов системы по отношению друг к другу или к имеющимся решениям.

Переход от документоцентризма к датацентризму. Различные описания системы не должны готовиться в форме отдельных документов. Все описания должны храниться в виде взаимосвязанных отдельных информационных единиц-данных, готовых для объединения в хранилищах информации. Работа с изменениями должна вестись в терминах отдельных данных, а не «документов».