

ОСОБЕННОСТИ УПРАВЛЕНИЯ ИНЖЕНЕРНОЙ ИНФРАСТРУКТУРОЙ НА ОСНОВЕ ИНТЕГРИРОВАННОЙ МОДЕЛИ ОБЪЕКТОВ И БИЗНЕС-ПРОЦЕССОВ

Гребенюк Г.Г., Калянов Г.Н., Ковалёв С.П., Лукинова О.В., Рошин А.А., Середа Л.А.

Институт проблем управления им. В.А. Трапезникова РАН, Москва, Россия
gggrebenuk@gmail.com, kalyanov@mail.ru, kovalyov@sibnet.ru, lobars@mail.ru, rochinaa@mail.ru,
lsereda123@gmail.com

Аннотация. Рассматриваются типичные ошибки в бизнес-процессах современного предприятия, связанные с информационными ресурсами и возникающие при некорректном построении последовательности бизнес-операций. Исследуется влияние ошибок в бизнес-процессах на работоспособность инженерной инфраструктуры. Комплексность проблемы потребовала создание интегрированной модели бизнес-процессов и моделей технического объекта, рассматриваются принципы создания и особенности представленной модели.

Ключевые слова: инженерная инфраструктура, инженерная сетевая система, бизнес-процесс, динамический анализ, статический анализ, ошибка в потоках данных, теория категорий.

Введение

Инженерная инфраструктура (ИНИ) представляет собой комплекс следующих составляющих:

- 1) Объект управления (ОУ): инженерная сетевая система (ИСС) – электрическая, тепловая, дорожная и др., посредством которой обеспечивается поставка потребителям основного ресурса.
- 2) Субъектом управления (СУ) является ресурсоснабжающая организация (РСО), обеспечивающая эксплуатацию ИСС таким образом, чтобы ей осуществлялась бесперебойная поставка основного ресурса потребителю.

Основная цель управления ИНИ, которая должна быть реализована бизнес-процессами (БП) РСО на стадии эксплуатации ИСС, – эффективная поставка ресурса потребителю. Основной стратегией, реализующей поставленную цель в рамках данной работы, является обеспечение высокой готовности ОУ. Это означает, что в случае отказа какого-либо компонента ИСС за счет безошибочно выстроенного управленческого процесса СУ гарантируется восстановление ее работоспособности в заданный период времени и на требуемом уровне. При этом если полностью работоспособный объект может обеспечивать максимальную эффективность своего применения, то эффективность частично работоспособного объекта в тех же условиях меньше максимально возможной, но остается выше допустимой. Уровень эффективности частично неработоспособного объекта ниже допустимого. Полностью неработоспособный объект применять по назначению невозможно.

Спецификой данной работы является тот факт, что задача управления ИНИ может быть решена на основе интеграции моделей ОУ и моделей управляющего бизнес-процесса. В качестве перспективного математического аппарата для унифицированного строгого формального представления моделей предлагается теория категорий.

Следует отметить, что влияние БП на технологические процессы или операции в ИНИ, может вызывать изменение состояний инженерной сетевой системы и ее работоспособности.

В данной работе авторы руководствуются терминами и определениями в области надежности [1]. Появление ошибки в БП может различным образом влиять на работоспособность ИНИ, которая определяется как состояние объекта, при котором он способен выполнять заданные функции, сохраняя значения основных параметров в пределах, установленных нормативно-технической документацией. К ним могут относиться показатели качества продукции, производительности, материальных и стоимостных затрат на изготовление продукции. Например, для объекта электроэнергетики такими параметрами являются частота электрического тока, напряжение на шинах источников питания и узлов нагрузки и степень удовлетворения потребности потребителей в электрической энергии.

Отметим, что наиболее типичными для бизнес-процессов современного предприятия (включая РСО) являются ошибки, связанные с информационными ресурсами (ошибки в потоках данных) и возникающие при некорректном построении последовательности бизнес-операций. Эти типы ошибок не всегда выявляются при тестировании и поэтому могут влиять на работоспособность физической системы (ИСС).

Практически отсутствуют исследования взаимосвязи ошибок бизнес-процессов и процессов в физических системах, подходы к оценкам возникающих негативных последствий. В тоже время эти последствия могут быть сравнимы с ущербом от хакерских атак на киберфизические системы, к которым относится и ИНИ. Благодаря специфике взаимодействий бизнес-процессов с объектом

управления, исследования в данной области отличаются новизной и представляют самостоятельный интерес для изучения.

1. Интегрированная модель объекта и бизнес-процесса

1.1. Общее описание интегрированной модели и ее уровни

На рис. 1 приведена схема взаимосвязи моделей предметной области, включающей в себя инженерную сетевую систему в качестве объекта управления и ресурсоснабжающую организацию (PCO) в качестве управляющей системы.

Моделирование предметной области включает два этапа – построение концептуальных и логических моделей, соответственно. На концептуальном уровне строится функциональная модель процессов PCO с использованием одного из наиболее популярных языков визуального моделирования IDEF0 или DFD [2], а также онтология предметной области [3]. На логическом уровне строятся три компонента интегрированной модели, служащей основой для анализа и верификации процессов управления ИСС: графовая (функциональная) модель бизнес-процессов, информационная модель предметной области с использованием диаграмм «сущность-связь» (ER-модель) [2], а также графовая модель инженерной сетевой системы.

Предлагаемая функциональная модель бизнес-процесса описывается на языке смешанных графов, является многоуровневой и включает в себя 3 взаимоувязанные компоненты: организационно-штатную структуру PCO, собственно модель бизнес-процесса, а также данные об обеспечивающих ресурсах различного вида (материальные, людские и т.п.). В качестве входной информации при построении графа используется модель бизнес-процессов PCO в виде иерархии DFD-диаграмм или IDEF0-диаграмм (при этом нет ограничений на использование какого-либо другого языка визуального функционального моделирования). На основании разработанных алгоритмов производится трансляция диаграмм в прототип графа и доработка этого прототипа вручную. При этом транслятор осуществляет преобразование иерархической модели в одноуровневый граф. Ручная доработка графа заключается в идентификации участков, которые могут выполняться параллельно, идентификации возможных вариантов продолжения (т.е. выбора бизнес-функции и указания ее возможных последователей) и т.п.

Информационная модель бизнес-процесса представляет собой диаграмму «сущность-связь» в нотации Баркера, сущности которой соответствуют объектам ИСС. Для ее построения и приведения к Третьей нормальной форме (3НФ) могут использоваться известные алгоритмы выделения сущностей предметной области из функциональной модели процесса (в частности, из DFD-диаграмм).

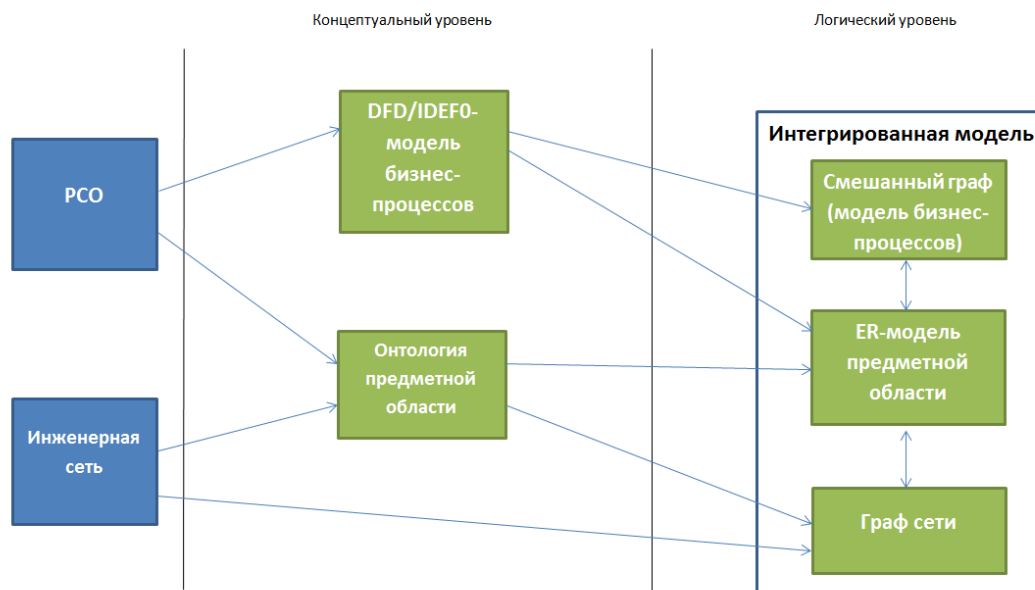


Рис. 1. Взаимосвязи моделей предметной области

Графовая модель инженерной сетевой системы описывает ее объекты и связи между ними (структуру системы).

1.2. Смешанный граф как модель бизнес-процесса

Как упоминалось выше, модель бизнес-процесса является многоуровневой. Нижний уровень модели содержит информационные объекты (ИО), представляемые с помощью кортежей $D_i(a_i^1, a_i^2, \dots, a_i^n)$, где D_i - идентификатор i -го ИО, a_i^j - j -ый атрибут i -го ИО.

Бизнес-операция моделируется парой $T_i D_j = (T_i, D_j)$, где T_i - тип операции с ИО. При этом выделяются следующие типы операций: создание, присваивание значений (определение), использование, определение прав доступа, архивирование, уничтожение, регистрация, ознакомление, редактирование, утверждение (визирование), согласование, публикация (для всеобщего доступа), передача на исполнение, привязка к другим ИО. При этом

$$T_i D_j = (T_i a_j^1, T_i a_j^2, \dots, T_i a_j^k), \quad (1)$$

однако для ряда операций (например, операции редактирования) могут существовать такие индексы m , что $T_i a_j^m = a_j^m$, т.е. операция может применяться не ко всем атрибутам ИО.

Бизнес-функция моделируется кортежем бизнес-операций

$$I_m((T_{1m}, D_{1l}), \dots, (T_{km}, D_{kl})), \quad (2)$$

где I_m – должность или фамилия исполнителя,

T_{1m}, \dots, T_{km} – элементы множества $\{T_i\}$,

D_{1l}, \dots, D_{kl} – элементы множества $\{D_j\}$.

При этом, не нарушая общности, можно считать, что внутри бизнес-функции бизнес-операции имеют естественный порядок исполнения.

Модель бизнес-процесса представляет собой граф управления бизнес-функциями

$$G(N, \{n_0\}, \{n_\phi\}, E, M, EM, EN, R, ER), \quad (3)$$

где N – множество узлов, каждый из которых соответствует бизнес-функции;

$\{n_0\}$ и $\{n_\phi\}$ – множества входных и завершающих узлов, соответственно;

E – множество управляющих ребер такое, что $\forall n_i, n_j \in N \cup \{n_0, n_\phi\}: (n_i, n_j) \in E$, если возможна ситуация, когда за выполнением бизнес-функции n_i будет выполняться бизнес-функция n_j ;

M – множество узлов, соответствующих структурным единицам предприятия (вплоть до роли конкретного исполнителя);

EM - множество ребер подчиненности такое, что $\forall m_i, m_j \in M: (m_i, m_j) \in EM$, если структурная единица m_i подчинена структурной единице m_j ;

EN – множество ребер исполнения бизнес-функции такое, что $\forall m_i \in M, n_j \in N: (m_i, n_j) \in EN$ если бизнес-функция n_j может быть выполнена в подразделении m_i ;

R – множество ресурсов предприятия;

ER – множество ребер использования ресурсов такое, что $\forall r_i \in R, n_j \in N: (r_i, n_j) \in ER$, если бизнес-функция n_j использует при своем выполнении ресурс r_i .

1.3. Граф инженерной сетевой системы

Модель инженерной сетевой системы представляет собой граф $G(V, E)$,

где V – множество объектов инженерной сетевой системы,

E – множество связей между объектами инженерной сетевой системы.

Множество V можно разделить на

V_s – подмножество объектов-источников ресурса (электростанции, месторождения нефти и газа и др.),

V_c – подмножество объектов-потребителей ресурса (промышленные предприятия, жилые дома и др.);

V_d – подмножество объектов инженерной сетевой системы, распределяющих или преобразующих ресурсы (распределительные, компрессорные и другие подстанции, линии электропередач, нефтепроводы и др.).

Следует отметить, что вершинами графа являются как точечные объекты сети (электростанции, подстанции, колодцы и др.), так и протяженные (участки трубопроводов, линий электропередачи и т.п.). Ребра графа отображают только соединения этих объектов между собой.

2. Методы анализа и верификации интегрированной модели

2.1. Понятие ошибки в потоках данных бизнес-процессов

Наиболее типичными для бизнес-процессов современного предприятия ошибками являются те, которые связаны с информационными ресурсами (ошибки в потоках данных) и возникают при некорректном построении последовательности бизнес-операций (создание, присваивание значений (определение), использование, определение прав доступа, архивирование, уничтожение, регистрация, ознакомление, редактирование, утверждение (визирование), согласование, публикация для всеобщего доступа, передача на исполнение, привязка к другим информационным объектам). Примерами таких ошибок являются:

- создание информационных объектов (ИО) и/или их атрибутов, не используемых в дальнейшей деятельности;
- отсутствие и/или неполнота ИО и/или их атрибутов;
- дублирование ИО и/или их атрибутов и, как следствие, их несогласованность и противоречивость и др.

Специфика данных ошибок для бизнес-процесса обуславливается наличием регламентов доступа к атрибутам ИО, запрещающих или ограничивающих доступ при выполнении ряда бизнес-операций. Так, например, такой атрибут сотрудника как его зарплата на ряде предприятий доступен только руководству и сотрудникам бухгалтерии.

Отметим, что ключевыми бизнес-операциями являются операции определения, использования и назначения прав доступа, остальные операции являются лишь вариациями вышеназванных. Исключение составляет операция привязки к другим информационным объектам, однако она может быть встроена в последовательность операций с помощью операций использования и определения обеих ИО (сначала того, к которому осуществляется привязка, а затем – привязываемого). Поэтому, не нарушая общности, в дальнейшем будем использовать три перечисленные выше операции.

Для обнаружения ошибок в потоках данных предлагается использование комплекса методов верификации процессов управления, базирующихся на теории зависимости по данным, а именно:

- метод генерации множества тестовых маршрутов (вариантов процесса управления), в совокупности гарантирующих обнаружение ошибок в потоках данных, а также позволяющих обнаруживать ошибки, выявление которых осуществляется известными методами тестирования, базирующимися на покрытии графа процесса;
- метод разбиения входных данных об авариях в сетях на «обнаруживающие подобласти», позволяющий сгенерировать множество входных тестов;
- метод статического анализа процессов управления, позволяющий обнаруживать различные типы «грубых» ошибок при исследовании графа процесса;
- метод динамического анализа вариантов процесса управления, позволяющий обнаруживать различные типы «тонких» ошибок при исследовании графа процесса.

2.2. Тестирование бизнес-процессов

Основной проблемой при планировании процедуры тестирования является проблема выбора критерия тестирования, т.е. задача выделения тех частей объекта, которые необходимо тестировать. Известные критерии тестирования и соответствующие алгоритмы выбора стратегий тестирования, основанные на анализе графовой модели объекта, не обеспечивают обнаружения рассматриваемых ошибок в потоках данных бизнес-процессов. Следовательно, при создании критерия тестирования бизнес-процесса необходимо учитывать не только его структуру управления, но и структуру его потоков данных.

Для целей тестирования введем трехуровневую модель. На первом уровне строится среда данных – множество всех определений всех аргументов бизнес-функции, для которых существует маршрут из точки входа в бизнес-процесс в рассматриваемую точку, на котором все элементы множества не переопределяются. На втором уровне строится контекст данных – множество наборов из n определений различных атрибутов, для которых существует маршрут из точки входа в бизнес-процесс в рассматриваемую точку, на котором все элементы набора принадлежат среде данных (т.е. не переопределяются). На третьем уровне строится упорядоченный контекст данных – множество упорядоченных наборов из n определений различных атрибутов, для которых существует маршрут из точки входа в бизнес-процесс в рассматриваемую точку, на котором все элементы набора принадлежат среде данных и выполняются в порядке, предписываемом данным набором.

Соответствующие критерии тестирования выглядят следующим образом [4]:

Критерий А требует, чтобы каждый элемент среды данных каждой бизнес-операции был проверен по крайней мере однажды.

Критерий Б требует, чтобы каждый элемент контекста данных каждой бизнес-операции был проверен по крайней мере однажды.

Критерий В требует, чтобы каждый элемент упорядоченного контекста данных каждой бизнес-операции был проверен по крайней мере однажды.

Для удобства исследования предложенных критериев пронумеруем их следующим образом: C_2 – критерий А, C_3 – критерий Б, C_4 – критерий В. Известные критерии тестирования, основанные на анализе графовой модели объекта и требующие проверки каждой ветви или каждого функционального узла (оператора) графа по крайней мере однажды, обозначим традиционно C_1 и C_0 , соответственно.

Пусть M^B – множество, элементами которого являются все возможные подмножества множества маршрутов в некотором бизнес-процессе B . Тот факт, что некоторое $M_k \in M^B$ удовлетворяет требованиям некоторого критерия тестирования C_i , обозначим следующим образом: $M_k \leftrightarrow C_i$.

Будем говорить, что некоторый ИО является определенным в бизнес-процессе, если на каждом использующем его маршруте, по крайней мере, одному из его атрибутов присваивается некоторое значение. Тогда для бизнес-процессов, в которых отсутствуют неопределенные и неиспользуемые ИО, а также конструкции типа skip, справедлива следующая теорема иерархии критериев [4]:

Теорема. Любое множество маршрутов $M_k \in M^B$, удовлетворяющее требованиям критерия C_i для $1 \leq i \leq 4$, также удовлетворяет и требованиям любого из критериев C_j при $1 \leq j < i$.

Таким образом, предложенные критерии тестирования позволяют:

- обеспечить обнаружение специфических для бизнес-процессов ошибок в потоках данных, связанных с их обработкой под различными масками, обеспечивающими регламенты доступа;
- обеспечить выявление всех тех ошибок, обнаружение которых может производиться с помощью традиционных критериев, основанных на анализе программных графов и применяемых к бизнес-процессам.

2.3. Статический анализ потоков данных бизнес-процессов

Метод статического анализа потоков данных основан на введении специальной дисциплины взаимодействия состояний информационных объектов (ИО) на любом этапе выполнения бизнес-процесса. Состояние ИО определяется последним обращением к нему и задается следующим образом:

$$S_i(A = (a_1, a_2, \dots, a_m)) = (i, Q = (q_1, q_2, \dots, q_m), D = (d_1, d_2, \dots, d_m)), \quad (4)$$

где i – номер узла графа бизнес-процесса;

q_j – тип обращения к j -му атрибуту ИО: $q_j \in \{w, r, n\}$, где w – определение атрибута, r – использование атрибута, n – отсутствие обращения к атрибуту;

d_j – элемент маски доступа к j -му атрибуту ИО: $d_j \in \{W, R, N\}$, где W – разрешение доступа на определение атрибута, R – разрешение доступа на использование атрибута, N – запрещение доступа к атрибуту.

Далее, не нарушая общности, будем считать, что ИО содержит единственный атрибут.

При анализе потоков данных основное внимание обращается на последовательность состояний ИО (т.е. фактически на последовательность определений/использований его атрибутов). Будем обозначать эту последовательность следующим образом:

$$d^{i1}q^{i1}d^{i2}q^{i2} \dots d^{ik}q^{ik} \quad (5)$$

где верхний индекс обозначает номер узла графа бизнес-процесса, в котором производится обращение к рассматриваемому ИО.

Для корректной работы бизнес-процесса по крайней мере должны удовлетворяться следующие 5 правил, касающихся построенной последовательности состояний ИО:

- 1) последовательность не должна содержать цепочек $\dots d^i q^i \dots$, в которых $d^i = N$, а $q^i \in \{w, r\}$;
- 2) последовательность не должна содержать цепочек $\dots d^i q^i \dots$, в которых $d^i = R$, а $q^i = w$;
- 3) $\forall i$ такого, что $(q^i = r) \wedge (d^i \neq N) \exists j < i$ такое, что $(q^j = w) \wedge (d^j = W)$.
- 4) $\forall i, j$, таких что $(q^i = w) \wedge (d^i = W) \wedge (q^j = w) \wedge (d^j = W) \exists i < k < j$, такое что $(q^k = r) \wedge (d^k \neq N)$.
- 5) $\forall i$ такого, что $(q^i = w) \wedge (d^i = W) \wedge (\neg \exists j > i, \text{ такого что } (q^j = w) \wedge (d^j = W)) \exists k > i$, такое что $(q^k = r) \wedge (d^k \neq N)$.

Нарушения перечисленных правил вызывают ошибки при выполнении бизнес-процесса (или, по крайней мере, являются симптомами ошибок) и могут происходить по следующим причинам:

- попытки использования неопределенных атрибутов ИО;
- повторные определения атрибутов без промежуточного их использования;
- некорректные определения прав доступа к ИО и их атрибутам;
- неиспользуемые ИО и/или их атрибуты;
- ошибки в маршрутизации ИО, приводящие к задержкам (например, график ремонта из-за неверной последовательности функций: формирование наряд-задания, накладных, заявок на запчасти);
- отсутствующие ИО и/или их атрибуты (например, уровень воды для плана восстановления после наводнения) и др.

2.4. Динамический анализ потоков ресурсов бизнес-процессов

Для целей динамического анализа в качестве модели ресурсов удобно использовать индексные множества, т.к. обычная интерпретация ресурса как пары (наименование, количество) не позволяет обнаруживать ошибки, связанные с их использованием. Под индексным множеством понимается пятерка

$$P(I, X, I, B, \Phi), \quad (6)$$

где I – множество индексов;

X – множество мест хранения данных о ресурсах («элементов памяти»), при этом $x \in X$ есть пара (x_1, x_2) , где x_1 – имя экземпляра сущности информационной модели предприятия (ER-модели), соответствующего конкретному ресурсу, x_2 – имя атрибута сущности, определяющего количество экземпляров ресурса данного вида;

$I: I \leftrightarrow X$ – взаимно-однозначное отображение идентификации;

B – множество допустимых состояний элементов памяти, разбивающееся на непересекающиеся классы состояний;

$\Phi: I \rightarrow B \cup \varepsilon$ – определяет допустимые состояния следующим образом (при этом f – функция классификации, ставящая в соответствие элементам каждого класса состояний определенное целое число, однозначно идентифицирующее данный класс):

$$\Phi(x) = \begin{cases} f(x_2), & \text{если } \exists j \in I: I(j) = x \\ \varepsilon & \text{в противном случае} \end{cases}. \quad (7)$$

Состояние индексного множества на любом этапе бизнес-процесса определяется последним обращением к нему и задается следующим образом:

$$S(P) = (n, Q, ACT), \quad (8)$$

где $n \in N$ (множество узлов бизнес-функций в графе управления бизнес-функциями);

Q – тип обращения (d – объявление, w – поступление на склад, r – получение со склада, b – бронирование, o – снятие брони);

ACT – права доступа к ресурсу исполнителя $m \in M$ (множество узлов исполнителей в графе управления бизнес-функциями), при этом $ACT(m, P)=1$, если доступ разрешен, и $ACT(m, P)=0$, в противном случае.

Задается семантика различных типов обращения к индексному множеству. Например, семантика объявлений для каждого индексного множества задает вводимые им объекты и заключается в следующем:

- 1) выбор множества индексов I для объекта P ;
- 2) выбор множества элементов памяти X ;
- 3) проверка $X \cap Y = \emptyset \forall Y$ для всех объявленных ранее объектов;
- 4) установление взаимно-однозначного соответствия $I: I \leftrightarrow X$;
- 5) обнуление всех элементов x_2 множества X ($\forall x=(x_1, x_2) \in X$) происходит установление $x_2=0$.

Предлагаемый метод динамического анализа потоков ресурсов основан на концепции абстрактной семантической машины, представляющей собой отладочный инструмент, работающий в автоматическом режиме. Эта машина моделирует бизнес-среду и способна в режиме интерпретации осуществлять выявление ошибок в потоках данных о ресурсах путем вызова соответствующих семантических подпрограмм.

Предложенный метод динамического анализа восходит к работам Венской школы [5, 6] и является одной из первых попыток описания семантики визуального языка моделирования для автоматического обнаружения семантических ошибок в бизнес-процессах.

3. Влияние ошибок бизнес-процессов на работоспособность инженерной инфраструктуры

На рис. 2 приведена технология использования разработанных методов анализа бизнес-процессов. Для анализа последствий ошибок БП (изменения работоспособности инженерной инфраструктуры) необходимо расширить представленный выше комплекс моделей, добавив модель склада обеспечивающих ресурсов и логико-дифференциальную модель технологических процессов. Таким образом, для решения данной задачи используются две основных модели: модель инженерной сетевой системы (модель ИСС) и модель бизнес-процесса РСО (модель БП). При этом в модель инженерной сетевой системы входит граф сетевой системы, модель склада и логико-дифференциальная модель технологических процессов, протекающих в объектах сети.

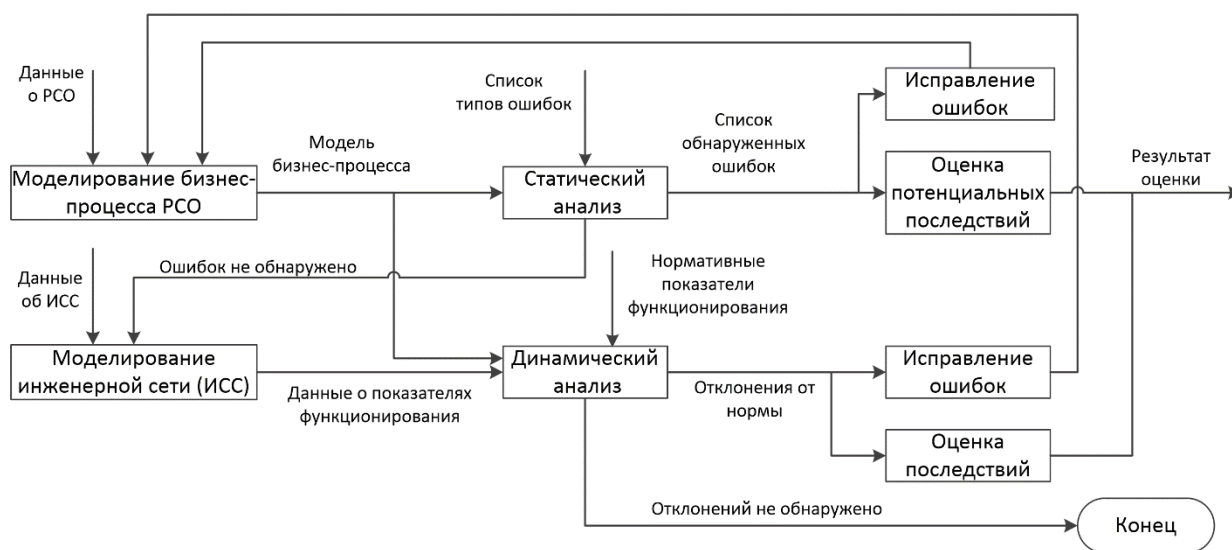


Рис. 2. Технология использования разработанных методов анализа бизнес-процессов

Для корректной работы инженерной инфраструктуры необходимо проверить модель БП на наличие статических и динамических ошибок в БП.

На первом этапе проводится моделирование бизнес-процесса в виде смешанного графа, строится множество маршрутов на этом графе, в совокупности обеспечивающих обнаружение ошибок в потоках данных. Для этого на вход блока моделирования БП поступают данные о структуре и деятельности РСО. Затем выполняется статический анализ потоков данных, для которого блок моделирования БП предоставляет данные об операциях (множество маршрутов тестирования). Если статическая ошибка найдена, то она исправляется путем модификации модели БП. Исправленная модель БП снова подвергается статическому анализу. Статические ошибки в потоках данных могут оказывать влияние на любой объект сети.

Если на этапе статического анализа ошибок не обнаружено, то выполняется динамический анализ. В отличие от статического анализа, при динамическом анализе используются модели ИСС. При этом блок моделирования ИСС отправляет основные показатели функционирования в блок динамического анализа для их сравнения с нормативными показателями. Обнаруженное расхождение сигнализирует о наличии динамических ошибок в БП. Если динамическая ошибка обнаружена, то она исправляется путем модификации модели БП. После модификации БП необходимо повторное проведение статического анализа. Динамические ошибки оказывают влияние на определенные подмножества объектов сети.

Если динамических ошибок не обнаружено, то анализ БП завершается.

И на этапе статического, и на этапе динамического анализа выполняется оценка последствий обнаруженных ошибок. Размер последствий может учитываться при принятии решения о

модификации БП РСО для исправления найденной ошибки т.к. модификация БП может быть связана с дополнительными затратами (наем персонала, закупка оборудования и т.д.).

Примеры статических и динамических ошибок и их возможные последствия приведены в таблице 1.

Таблица 1. Ошибки бизнес-процесса и их последствия

Пример ошибки	Тип ошибки	Последствия
Отсутствие в БП операции по ТО объекта, входящего в состав системы	Статическая	Задержка ТО и прямая возможность отказа, снижение эффективности функционирования ниже допустимого уровня.
Отсутствие в БП операции для аварийного ремонта объекта, входящего в состав системы	Статическая	Прямая задержка ремонта объекта.
Отсутствие в БП операции пополнения запасов на складе	Статическая	Задержка ТО и прямая возможность отказа и снижения эффективности функционирования.
Отсутствие данных об одном из основных параметров, определяющих работоспособность и режим работы	Статическая	Прямая задержка ремонта объекта, возможность снижения эффективности.
Нехватка запасов какого-то изделия на складе (например, вследствие большей регламентированной интенсивности отказов)	Динамическая	Задержка ремонта, возможность снижения эффективности.
Нехватка ресурсов (людских, технических, инструментальных) для выполнения ремонтных работ (например, вследствие большей регламентированной интенсивности отказов)	Динамическая	Потенциальная возможность аварии при отказе с задержкой восстановления, возможность снижения эффективности.

Из таблицы 1 видно, что основные последствия связаны с прямыми или потенциальными (при определенных условиях) возможностями перехода из работоспособного в частично работоспособное или частично неработоспособное состояние.

Как сказано во Введении, объект может иметь 4 состояния (не считая предельного): работоспособное, частично работоспособное, частично неработоспособное, не работоспособное. Три первых состояния отличаются уровнем эффективности функционирования системы, соответственно, максимально возможным (высокий), выше допустимого (средний), ниже допустимого (низкий).

Таким образом, уровень эффективности функционирования системы может быть принят в качестве оценки последствий ошибок БП. Часто ущерб из-за отказов и снижения работоспособности описывается сокращением выпуска продукции и объема услуг, предоставляемых системой. В этом случае считается, что сокращение выпуска вызывается снижением производительности системы, в том числе вследствие ошибки БП.

Для оценки сокращения выпуска продукции и объема услуг используем такой показатель, как время восстановления – время, затрачиваемое непосредственно на выполнение операций по восстановлению объекта [1]. Ошибка в БП, вызывающая запаздывание времени начала восстановления (времени до восстановления), которое определяется временем от момента отказа до восстановления работоспособного состояния объекта, приводит к недовыпуску продукции или услуг системой на интервале времени, определяемым этим запаздыванием. Объем потерь определяется интегралом от потери производительности за период, равный запаздыванию.

В случае, если ошибка в БП вызывает прямой переход в частично работоспособное или частично неработоспособное состояние, то ущерб из-за недовыпуска продукции или услуг системой, определяется интегралом от потери производительности за период, равный времени восстановления.

4. Развитие методов моделирования инженерной инфраструктуры с применением теории категорий

Для сложных технических объектов, таких как инженерная инфраструктура, трудоемкой задачей может быть сборка целостной корректной модели из моделей составляющих. Фактически, требуется виртуально воспроизвести процесс строительства инженерной инфраструктуры на информационных и математических моделях. Перспективный подход к решению этой задачи развивается в течение ряда лет на базе алгебраического аппарата теории категорий [7 и др.]. Рассматриваются категории, объектами которых служат алгебраические представления моделей системных единиц различного уровня (от деталей до систем), построенные при помощи некоторого формализма, а морфизмы

описывают на языке этого формализма всевозможные действия, применяемые при сборке моделей сложных единиц из моделей составных частей. Ясно, что так действительно получаются категории, поскольку в них имеется композиция морфизмов (последовательное выполнение действий) и тождественные морфизмы (холостое «ничегонеделание» с любым представлением). Например, графы инженерных сетевых систем находятся в подходящей категории графов, а рассмотренные выше процессы, выполняемые на инженерной инфраструктуре, можно описать в рамках категории помеченных частично упорядоченных множеств **Pomset**.

Структурная схема объекта представляется диаграммой в категории вышеописанного вида. Для подходящей диаграммы можно построить универсальную конструкцию копредела (colimit) – алгебраический аналог сборки объекта из частей. Понятие копредела выражает в алгебраических терминах общепринятый взгляд на систему как на «контейнер», который включает в себя все части с учетом их структурных взаимосвязей, и ничего другого. Формально, копредел – это объект, снабженный морфизмами из каждой вершины диаграммы (ребрами), удовлетворяющими определенным условиям естественности и универсальности. Практическую значимость имеют и обратные задачи моделирования инженерной инфраструктуры, состоящие в поиске вариантов структуры объекта, (суб-, Парето-) оптимальных с точки зрения целевых функций его потребительского качества, таких как стоимость владения, производительность или надежность.

Мощный аппарат для манипулирования с диаграммами предоставляют конструкции, связанные с известной монадой диаграмм в «категории всех категорий» **CAT** [8]. Напомним, что эта монада порождается функтором конструирования категории диаграмм $\mathbf{D} : \mathbf{CAT} \rightarrow \mathbf{CAT}$, переводящим произвольную категорию C в категорию диаграмм \mathbf{DC} , в которой морфизмом диаграммы $\Delta : X \rightarrow C$ в $\Xi : Y \rightarrow C$ (где X, Y – малые категории) служит любая пара вида $\langle \gamma, fd \rangle$, состоящая из функтора $fd : X \rightarrow Y$ и естественного преобразования $\gamma : \Delta \rightarrow \Xi \circ fd$. Любой функтор $F : C \rightarrow D$ порождает функтор $F \circ - : \mathbf{DC} \rightarrow \mathbf{DD}$, переводящий диаграмму Δ в $F \circ \Delta$. Единица монады диаграмм состоит из компонент вида $\lceil _ \rceil : C \rightarrow \mathbf{DC}$, сопоставляющих объекту $A \in \text{Ob } C$ диаграмму-точку $\lceil A \rceil : I \rightarrow C$, где I – сингулярная категория, состоящая из одного объекта и его тождественного морфизма. Умножение в монаде диаграмм \mathbf{K} представляет собой «отрисовку» \mathbf{DC} -диаграммы в виде C -диаграммы: для диаграммы $\Xi : I \rightarrow \mathbf{DC}$ отрисовка $\mathbf{K}\Xi : \text{dom } \mathbf{K}\Xi \rightarrow C$ строится путем замены каждой точки $i \in \text{Ob } I$ C -диаграммой Ξi и разделения каждого морфизма диаграмм $\Xi k, k \in \text{Mor } I$, на составляющие его морфизмы из категории C . Отрисовка является частным случаем уплощающей конструкции Гротендика (Grothendieck flattening construction [9, п.12.2.10]).

Интерес представляют алгебры монады диаграмм – функторы вида $a : \mathbf{DC} \rightarrow C$, связанные определенными соотношениями с компонентами единицы и умножения монады. Например, если компонента единицы имеет левый сопряженный функтор (а правого сопряженного она иметь не может), то единица этого сопряжения состоит из копределов C -диаграмм, так что категория C кополна и, более того, указанный левый сопряженный $\text{colim} : \mathbf{DC} \rightarrow C$ задает алгебру. А при помощи отрисовки можно строить и другие алгебры, не изоморфные ни копределам, ни свободным алгебрам монады диаграмм.

В приложениях к моделированию инженерной инфраструктуры, подходящие подкатегории в \mathbf{DC} могут выступать в качестве пространств проектирования (design space) – областей поисковой оптимизации для решения обратных задач. Для этого целевые функции оптимизации преобразуются в функторы, действующие из пространств проектирования в линейно упорядоченные множества значений, рассматриваемые как категории. Для эффективной навигации в пространствах проектирования вдоль морфизмов диаграмм могут привлекаться средства компьютерной алгебры. Открывается возможность реализации высокоавтоматизированных технологий типа порождающего проектирования (generative design) для сложных систем.

Что касается приложений монады диаграмм, то компонента ее единицы задает представление любого объекта как бесструктурной сингулярной системы, а левый сопряженный к ней (при его наличии) представляет сборку систем в цельные объекты. Конструкция отрисовки строит детальную «плоскую» структуру многоуровневых систем, состоящих из систем (systems of systems, SoS), путем разрешения взаимосвязей верхнего уровня, причем ассоциативность умножения монады гарантирует независимость итоговой структуры от порядка анализа промежуточных уровней. Алгебры монады диаграмм задают шаблоны процедур «упаковки» структур систем в сложные объекты с соблюдением условий естественности относительно модификаций. Из математического «материала» монады диаграмм строятся и другие конструкции.

5. Заключение

Инженерная инфраструктура является сложной организационно-технической системой. Основные направления исследований в области неработоспособности сложных инженерных сетевых систем связаны с поиском критических элементов (уязвимостей), оценкой взаимовлияния объектов и процессов с использованием модели экономического баланса, анализом и оценкой устойчивости к деструктивным воздействиям внутренней и внешней природы и др. Взаимовлияние организационной и физической компонент исследуется при анализе устойчивости в части управления финансами, ремонтными средствами и др. в периоды предотвращения последствий за счет повышения надежности и восстановления системы после деградации с целью минимизации стоимости и сроков ремонта.

Проведенное исследование показывает важность анализа влияния бизнес-процессов и управляемой ими физической системы в процессе текущей эксплуатации. Показано, что негативные последствия этого влияния могут проявляться в результате ошибок в БП или в данных, поступающих из физической системы, и выражаться в нарушении работоспособности системы, снижении эффективности производства продукции и услуг.

Литература

1. ГОСТ Р 27.102-2021 “Надежность в технике. Надежность объекта. Термины и определения” – М.: Стандартиформ, 2021. – 46 с.
2. Блюмин А.М., Калянов Г.Н. Проектирование информационных систем. – М.: Горячая линия - Телеком, 2022. – 361 с.
3. Гребенюк Г.Г., Калянов Г.Н., Ковалёв С.П., Крыгин А.А., Лукинова О.В., Никишов С.М. Модели и методы управления технологической инфраструктурой на базе цифровых двойников // Управление развитием крупномасштабных систем (MLSD’2021): труды Четырнадцатой междунар. конф – М.: ИПУ РАН, 2021. – С. 834–845.
4. Калянов Г.Н. Теория бизнес-процессов. - М.: Горячая линия - Телеком, 2023. – 426 с.
5. Оллонгрен А. Определение языков программирования интерпретирующими автоматами. – М.: Мир, 1977. – 288 с.
6. Семантика языков программирования (сборник статей). – М.: Мир, 1980. – 395 с.
7. Ковалёв С. П. Теория категорий как математическая прагматика модельно-ориентированной системной инженерии // Информатика и ее применения. 2018. Т. 12, вып. 1. – С. 95–104.
8. Guitart R., van den Bril L. Décompositions et lax-complétions // Cahiers de Topologie et Géométrie Différentielle Catégoriques. – 1977. – Vol. 19, No. 4. – P. 333–407.
9. Barr M., Wells C. Category theory for computing science. – London: Prentice Hall, 1990. – 538 p.