Северо-Казахстанский университет им. М. Козыбаева

УДК 004.942+004.414.23

На правах рукописи

ОСПАНОВА ГУЛЬМИРА ЖАБАЕВНА

Информационно-аналитическая система контроля целостности нормативной базы

6D075100 – Информатика, вычислительная техника и управление

Диссертация на соискание степени
доктора философии (PhD)

Научные консультанты
кандидат технических наук,
доцент
Е.В. Кухаренко

кандидат физико-математических наук,
доцент
О.В. Григоренко

Республика Казахстан
Петропавловск, 2024

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

БД – база данных
БНД – база нормативных документов
Д – данные
ДОУ – документационное обеспечение управления
ИБ – информационная безопасность
ИР – информационный ресурс
ИС – информационная система
Н – нормы
НСД – несанкционированный доступ
НД – нормативный документ
ОРД – организационно-распорядительные документы
ОСТ – отраслевой стандарт
ПР – правила
Р – рекомендации
СП – свод правил
СТНИО – стандарт научно-технических и инженерных объединений
СТО – стандарт организации
СУП – система управления предприятием
СЭД – система электронного документооборота
ТР – технический регламент
ТУ – технические условия
ЦИ – целостность информации
ЭЦП – электронная цифровая подпись
BPM – Business Process Management
CUA – Central User Administration
ECM – Enterprise Content Management
ERP – Enterprise Resource Planning
SNC – Secure Network Communications
SSF – Secure Store and Forward
SSL – Secure Sockets Layer
TLS – Transport Layer Security
VPN – Virtual Private Network

ВВЕДЕНИЕ

В современном мире существует огромное количество различных законов, правил и стандартов, которые регулируют различные сферы деятельности, однако со временем эти нормы могут устаревать или становиться неактуальными из-за изменений в обществе или технологическом прогрессе. Система поддержания целостности нормативной базы позволяет отслеживать все изменения в нормативной базе и своевременно обновлять соответствующие документы, что помогает организациям соблюдать требования закона и избегать возможных штрафов или других негативных последствий.

Кроме того, такая система может значительно упростить процесс работы с нормативными документами для сотрудников компаний, так как она предоставляет им быстрый доступ к необходимой информации и повышает эффективность управления бизнес-процессами. В целом, разработка системы поддержания целостности нормативной базы является важной задачей для обеспечения эффективного функционирования организаций и соблюдения ими всех требований, предъявляемых к организации и сопровождению бизнес-процессов.

Таким образом, **актуальность темы исследования** обусловлена следующими параметрами и показателями сопровождения и управления бизнес-процессами:

– противоречивость значений параметров управления процессами, установленных разными документами;

– отсутствие стратегии поддержания целостности базы нормативных документов;

– отсутствие однозначно регламентированного процессного подхода к управлению базой нормативных документов и бизнес-процессами;

– отсутствие обратной связи между объектами и субъектами базы нормативных документов в управлении бизнес-процессами;

– детерминированность процессов, регламентируемых базой нормативных документов, а также отсутствие резервов ресурсов.

Целью исследования является разработка моделей и методов контроля целостности и управления процессами внесения изменений в базу нормативных документов для обеспечения ее гарантоспособности и систематизации нормативных документов посредством придания свойства целостности базе нормативных документов.

Для достижения цели исследования поставлены следующие **задачи исследования**:

– разработать модели обеспечения контроля целостности базы нормативных документов;

– разработать методы обеспечения неизменности, определения субъектов информационной системы и достоверности состава, содержания и взаимодействия нормативных документов;

– разработать достаточные условия для выполнимости требований методов обеспечения неизменности, определения субъектов информационной системы и достоверности состава, содержания и взаимодействия нормативных документов;

– разработать алгоритмы реализации методов обеспечения неизменности, определения субъектов информационной системы и достоверности состава, содержания и взаимодействия нормативных документов;

– разработать модели информационно-аналитической системы контроля целостности базы нормативных документов как результат взаимно-однозначного (биективного) отображения фреймовых моделей представления базы нормативных документов в элементы проектируемой системы.

Объектом исследования является база нормативных документов как компонент системы сопровождения бизнес-процессов, реализующий и генерирующий управляющие и регламентирующие воздействия и сигналы на бизнес-процесс.

Предметом исследования рассматривается **обеспечение** гарантоспособности базы нормативных документов посредством придания свойства целостности базе нормативных документов, регламентирующих различные бизнес-процессы, и являющиеся представителями как субъектов, так и объектов в базе нормативных документов.

Научная новизна заключается в применении формализованного подхода к решению задачи обеспечения контроля целостности базы нормативных документов, рассматриваемая как объект и субъект управления в бизнес-процессах, в частности:

– использование алгебры предикатов для постановки задачи и формирования агрегированной модели обеспечения контроля целостности базы нормативных документов;

– разработка декларативных фреймовых моделей и методов обеспечения контроля целостности;

– использование семантических моделей для формализации представления базы нормативных документов.

Практическая значимость обусловлена эффектом от внедрения разработанных моделей и методов:

– придание согласованности документам в базе нормативных документов повысит управляемость процессов за счет более строгой и однозначной регламентации бизнес-процессов в нормативных документах;

– определенность санкционированных пользователей и сервисов позволит сформировать стратегию контроля целостности базы нормативных документов, что поможет обеспечить каскадное обновление документов;

– формализация связей между нормативными документами позволит реализовать взаимодействие документов между собой для формирования обратной связи в управлении бизнес-процессами;

– уменьшение вариативности в параметрах управления бизнес-процессами позволит снизить энтропию самой базы нормативных документов, за счет чего повысить жесткость и детерминированность процессов, регламентируемых базой нормативных документов.

По результатам диссертационного исследования **на защиту выносятся:**

– предикатная модель задачи обеспечения целостности базы нормативных документов, далее формализуемая фреймовой моделью нормативного документа и базы нормативных документов;

– методы определения субъектов информационной системы, имеющих права изменять базу нормативных документов; обеспечения неизменности состава, содержания и взаимодействия нормативного документа с другими нормативными документами, входящими в базу нормативных документов; определения достоверности состава, содержания и взаимодействия нормативного документа с другими нормативными документами, входящими в базу нормативных документов;

– модели информационно-аналитической системы контроля целостности базы нормативных документов.

Апробация работы проводилась на международной конференции «Global science and innovations 2019: Central Asia» (2019), международной научно-практической конференции "Стандартизация - инструмент повышения конкурентноспособности и интеграции казахстанской продукции в мировую экономику"(2019).

По теме исследования **опубликовано** 6 работ, из которых 3 статьи опубликованы в научных изданиях, включенных в Перечень научных изданий, рекомендуемых для публикации основных результатов научной деятельности, утверждаемый уполномоченным органом, в 1 статье – в международном рецензируемом научном журнале, имеющем ненулевой импакт-фактор (индексированном в базе данных Scopus), а также в материалах двух международных конференций. По результатам исследования получено авторское свидетельство на объект интеллектуальной собственности.

Личный вклад автора заключается в разработке основных теоретических и прикладных положений диссертационного исследования. Участие автора в совместных публикациях состоит в формализации постановки задач, моделей и методов придания целостности базе нормативных документов, а также моделей функционирования информационно-аналитической системы обеспечения целостности базы нормативных документов.

Структура диссертации. Диссертация имеет классическую структуру: введение, основная часть (три раздела), заключение, список использованных источников. Работа изложена на 103 страницах компьютерного текста, содержит 18 рисунков, 3 таблицы, 109 наименований библиографических источников.

Во введении приведены и обоснованы актуальность, цель и задачи, объект и предмет диссертационного исследования, представлены научная новизна и практическая значимость.

В первом разделе проведен анализ современного состояния проблемы обеспечения целостности информации (данных) в информационной системе предприятия и, в частности, нормативного документа как подмножества всех документов в базе нормативных документов. Проанализированы особенности базы нормативных документов, основные подходы к обеспечению целостности данных и информации, теоретические и прикладные исследования в области обеспечения целостности информации.

Во втором разделе выполнена постановка задачи обеспечения целостности базы нормативных документов, разработаны фреймовые модели нормативного документа и базы нормативных документов. Приведены модели и методы, а также обоснована достаточность фреймовых моделей для использования в решении задачи методами, предложенными в данной главе – метода определения субъектов информационной системы, имеющих право изменять базу нормативных документов, метода обеспечения неизменности и состава, содержания и взаимодействия, метода определения достоверности базы нормативных документов. Фреймовые модели представляют собой объект, на который получено свидетельство об авторском праве (Приложение А).

В третьем разделе представлена модель информационной технологии обеспечения целостности базы нормативных документов. Разработаны в соответствии с методами алгоритмы и модели решения подзадач определения субъектов информационной системы, имеющих право изменять базу нормативных документов, обеспечения неизменности и состава, содержания и взаимодействия, определения достоверности базы нормативных документов,

В заключении подведены итоги диссертационного исследования, содержащие основные выводы работы.

1 АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ К ОБЕСПЕЧЕНИЮ ЦЕЛОСТНОСТИ НОРМАТИВНОЙ ДОКУМЕНТАЦИИ

1.1 Анализ основных особенностей базы нормативных документов предприятия

Функционирующие в рыночной среде компании организуют свои бизнес-процессы таким образом, чтобы обеспечить стабильность работы и получение максимально дохода. Однако в современных условиях предприятие, которое, согласно [1, 2], создается с целью получения прибыли через удовлетворение потребностей рынка, или осуществления специальных социально значимых функций, является сложной системой и не может функционировать без четко определенных базовых правил, норм, которые касаются принципов качества продукции, безопасности и эффективности производства и иных процессов.

Определяют и фиксируют данные наборы правил и характеристик нормативные документы.

Как указано в [3], нормативный документ (НД) – это документ, устанавливающий правила, общие принципы или характеристики, касающиеся различных видов деятельности или их результатов.

В НД содержатся принципы и конкретные правила организации и выполнения процессов, отдельных работ и услуг, результаты которых обеспечивают стабильную работу предприятия и экономический эффект. Применяются такие документы, как в деятельности производственных предприятий**,** так и в организациях, которые занимаются оказанием услуг и выполнением работ.

Термин «НД», таким образом, можно представить, как обобщение, которое объединяет в себе различные виды документов, содержащих правила, нормы, условия и другую важную для осуществления различных видов деятельности информацию.

Состав НД предприятия зависит от его масштабов и сферы деятельности.

Важным и одним из наиболее часто применяемых в работе предприятия видом НД, являются стандарты разных уровней.

На территории конкретной страны, в соответствии с ГОСТами [3, с. 2-38; 4, 5], а также [6-9], действуют следующие НД в виде стандартов:

– национальные стандарты (принятые уполномоченным органом по стандартизации на уровне государства, например, ГОСТ Р);

– международные стандарты (принятые международными организациями, например, ИСО/МЭК);

– межгосударственные стандарты (принятые Евразийским советом по стандартизации и странами СНГ, обозначаются как ГОСТ);

– региональные стандарты (действие распространяется на страны конкретного географического региона, которые согласовали данный стандарт);

– регламенты (в том числе технические регламенты (ТР), которые приняты на уровне международных договоров, либо органами власти и устанавливают обязательные требования к продукции и процессам);

– правила (ПР) по стандартизации (обязательны для применения, дополняют и конкретизируют положения национального стандарта);

– рекомендации (Р) по стандартизации (добровольны для применения, содержат советы организационно-методического характера);

– нормы (Н) (устанавливают количественные и качественные критерии);

– своды правил (СП) (ПР и Н разработанные органами исполнительной власти могут объединяться в своды правил, которые содержат технические правила и описание процессов для всего жизненного цикла продукции);

– классификаторы технико-экономической информации (НД, которые классифицируют, распределяют и кодируют информацию для создания государственных информационных систем и ресурсов);

– стандарты организаций (СТО) (НД организаций, применяемые для совершенствования производственного и иных процессов, выполнения работ и услуг, распространения полученных результатов);

– стандарты научно-технических и инженерных объединений (СТНИО) (разрабатывается для добровольного применения, как правило, на инновационные виды продукции и процессов с целью распространения информации о передовых достижениях);

– технические условия (ТУ) (устанавливают технические требования к продукции и процессам, считаются НД, если на них содержатся ссылки в договорах на поставку).

Некоторые источники [7, с. 3-670; 8, с. 3-160] выделяют также отраслевые стандарты (ОСТ), которые разрабатываются министерствами применительно к продукции конкретных отраслей и подведомственным предприятиям. Однако упоминается ОСТ все реже в связи с ориентацией национального законодательства и терминологии на международную практику [10].

По мнению [11], «цель стандартизации – выявление наиболее правильного и экономичного варианта, т.е. нахождение оптимального решения», а также «общей целью стандартизации является защита интересов потребителей и государства по вопросам качества продукции, процессов и услуг». Если объединить эти определения и распространить их на НД предприятия, то можно сказать что они разрабатываются с целью обеспечения максимально рациональной, безопасной и эффективной организации бизнес-процессов, а также соблюдения законных интересов государства, производителей и потребителей продукции.

Среди бизнес-процессов предприятия, согласно [12, 13] выделяют:

– основные бизнес-процессы (преобразование ресурсов в продукт для потребителя и формирование дохода);

– обеспечивающие (поддерживающие) бизнес-процессы (поставляют необходимые для преобразования ресурсы, обеспечивают функционирование инфраструктуры);

– процессы управления (предоставляет ресурсы по управлению всеми бизнес-процессами);

– процессы развития (нацелены на перспективу, обеспечивают развитие технологий, совершенствование продукции, инновации).

Важно отметить, что в ходе выполнения и организации выделенных групп бизнес-процессов предприятие сталкивается с множеством НД, которые можно условно разделить на две группы. НД первой группы (внешние НД) формируются, утверждаются, устанавливаются и действуют извне в виде регулирующих и унифицирующих норм. К внешним НД можно отнести ТР, ГОСТы, ОСТ, ПР, Р, Н и иные регулирующие документы, утвержденные на межгосударственном, региональном, национальном и административно-территориальном уровнях.

НД второй группы (внутренние НД) разрабатываются и используются самим предприятием. Внутренние НД формируются с учетом вышестоящих внешних НД и не должны им противоречить. К внутренним НД относятся ТУ, СТО, СТНИО для инновационных продуктов, различные положения, инструкции, рецептуры и т.п.

Схема взаимосвязи внешних и внутренних НД и их влияния на бизнес-процессы предприятия представлена на рисунке 1.1.

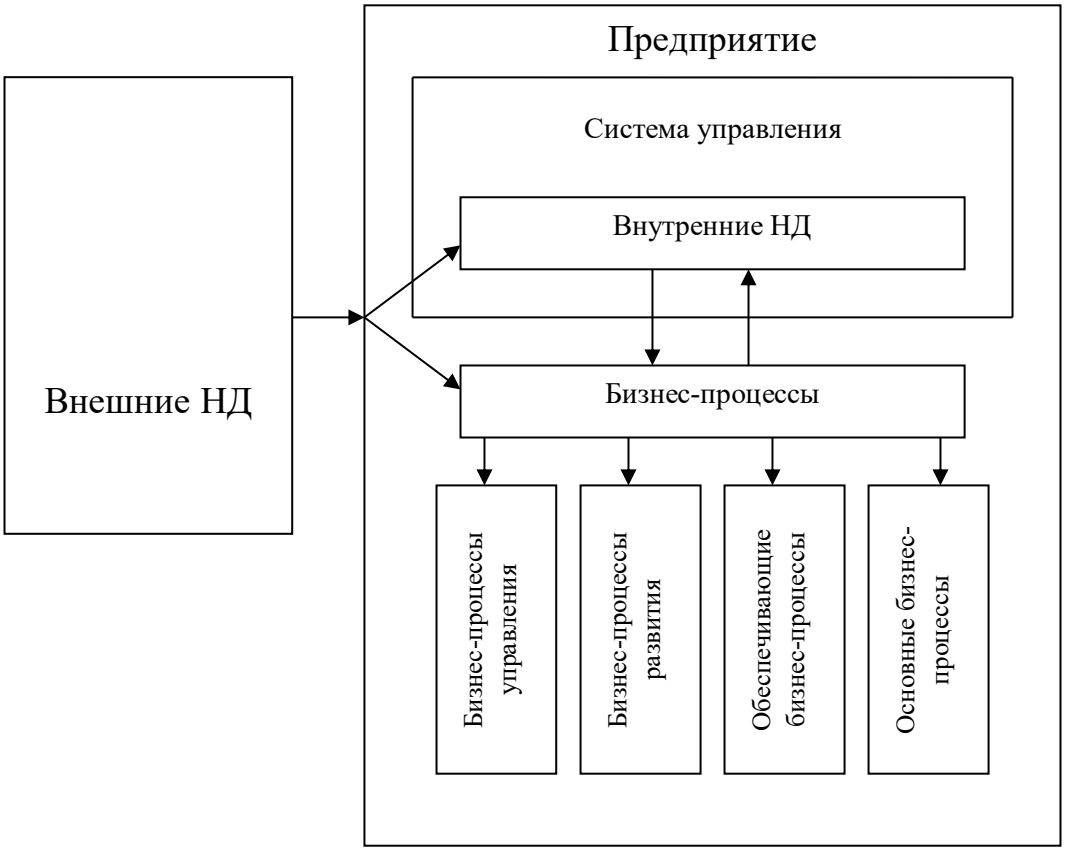

Рисунок 1.1 – Схема взаимосвязи внешних и внутренних нормативных документов, и их влияния на бизнес-процессы предприятия

Внешние НД, обладающие необходимой юридической силой, могут содержаться в виде действующих межгосударственных или региональных документов. На национальном уровне такие НД утверждает и издает государство в рамках задач регулирования документационного обеспечения управления (ДОУ).

Согласно [14], эти документы решают также следующие задачи:

– информационное обеспечение принимаемых решений на различных уровнях управления;

– реализацию прав и интересов граждан;

– взаимодействие государственных органов и организаций различных отраслей, а также контроль их деятельности;

– формирование качественного архивного фонда.

Если продукция или деятельность попадает под действие обязательных к применению внешних НД (стандарта, регламента и т.п.), то предприятие должно исполнять их требования и соблюдать нормы.

Внутренние НД предприятие разрабатывает самостоятельно, с учетом и на основе вышестоящих внешних НД. Они необходимы для обеспечения процесса управления, стабильного выпуска качественной и безопасной продукции, соблюдения определенных режимов и норм в различных процессах и услугах предприятия, обеспечения этих процессов соответствующими ресурсами. В данных НД содержится информация, которая используется для организации производственного и технологического процессов, эффективной реализации, безопасных условий транспортировки, хранения, эксплуатации и утилизации готового продукта.

В частности, согласно [5, с. 2-7], внутренние НД (стандарты) могут разрабатываться на:

– составные части продукции, инструмент и оснащение;

– процессы менеджмента;

– технологические процессы, а также нормы и требования с учетом обеспечения безопасности граждан, окружающей среды и имущества;

– методы и методики проектирования, проведения испытаний, измерений и/или анализа;

– услуги, оказываемые внутри организации;

– номенклатуру сырья, материалов, комплектующих;

– принципиально новые виды продукции, методы испытаний и управления производством.

– процессы выполнения работ на всех стадиях жизненного цикла продукции и др.

Кроме стандартов к НД относятся некоторые организационно-распорядительные документы (ОРД), а именно те из них, которые устанавливают принципы и правила организации деятельности компании и отдельных процессов. В зависимости от уровня принятия ОРД, так же как и стандарты, могут быть как внешними по отношению к предприятию (например,

принятые на национальном уровне), так и внутренними (принятыми внутри организации).

ОРД обеспечивают, регулируют и координируют организацию процессов управления деятельностью предприятия [15, 16]. Распорядительными документами оформляются управленческие решения, они включают: приказы, распоряжения, указания, постановления, решения. Организационные документы определяют статус и сферу деятельности предприятия и его подразделений, к ним относят: устав, положения, инструкции по видам деятельности, штатное расписание, правила и другие регламентирующие документы.

НД отличаются от остальных видов документов, которые обращаются на предприятии. Основное отличие НД является следствием определения из [3, с. 7-10]. НД устанавливают правила и принципы различных видов деятельности и их результатов. Тогда как другие документы фиксируют и констатируют определенную информацию, с целью накопления статистических данных, хранения, донесения конкретной информации до целевых групп пользователей, в иных целях.

Например, сопроводительные документы на товар, в отличие от НД, содержат констатирующую информацию о характеристиках товаров и товарных партий (ассортименте, количестве, цене, особенностях эксплуатации и т.д.), с которой может ознакомиться покупатель, либо другой заинтересованный пользователь. Или другой вид документов, по [17] – отчеты, в установленной форме содержат итоговые результаты обработки и анализа статистических данных за определенный период времени и тоже не являются НД. Также не устанавливает правил и принципов группа информационно-справочной документации, которую относят к ОРД [18].

На внешние НД предприятие не оказывает непосредственного влияния, поэтому просто соблюдает действующие требования и отслеживает их изменения с соответственной актуализацией внутренних НД.

Внутренние НД предприятие использует как инструмент установки и регулирования организационных, финансовых, календарно-плановых нормативов, характеристик готовой продукции, норм расхода ресурсов, использования оборудования, оптимального уровня складских запасов и т.п.

Совокупность НД, которые регулируют деятельность предприятия, в комплексе представляют собой его базу нормативных документов (БНД).

Как уже отмечалось, значительную часть НД предприятия составляют стандарты разных уровней разработки и утверждения. В результате анализа принципов стандартизации по [19, 20], а также сущности и состава соответствующих ОРД, становится возможным выделение таких особенностей БНД:

– законность (НД составляющие БНД предприятия не должны нарушать законодательные нормы, а также обязательные требования государственных, отраслевых и прочих стандартов);

– актуальность (все нормы и требования, которым соответствуют НД, должны быть действующими; кроме того, НД должны отвечать современным рыночным тенденциям, с учетом научно-технического прогресса);

– точность (все правила, описанные в НД предприятия, должны быть точно сформулированы и не должны допускать различных трактовок и дублирования);

– системность (составляющие БНД должны рассматриваться в системной взаимосвязи и быть совместимыми для эффективного планирования, анализа и управления);

– непротиворечивость (составляющие БНД элементы не должны противоречить внешним регулирующим правилам и друг другу, а их применение не должно препятствовать производственному процессу и экономической деятельности предприятия);

– сбалансированность (БНД должна одновременно соответствовать требованиям регулирующих органов, а также отвечать законным интересам самого предприятия и потребителей его продукции);

– адаптивность (БНД должна быть динамичной и своевременно адаптироваться к корректирующим факторам).

– эффективность (БНД должна соответствовать принципам эффективности, т.е. должна способствовать получению экономического (экономия ресурсов, повышение надежности), либо социального (обеспечение безопасности) эффекта);

– комплексность (НД на готовую продукцию должны рассматриваться в комплексе и быть связаны с НД на все ее составляющие (детали, полуфабрикаты, сырье, методы производства));

– доступность (информация, содержащаяся в НД должна быть максимально доступной имеющим соответствующий допуск лицам);

– контролируемость (БНД должна предоставлять возможности для эффективного всестороннего контроля).

Успешное управление во многом зависит от эффективности системы информационного обеспечения, которая выстроена на конкретном предприятии. БНД является важной и неотъемлемой частью такой системы. Соответственно для корректной и эффективной работы в условиях современного предприятия с учетом выделенных особенностей БНД, необходимо создание и реализация специальных технологий. Одной из таких технологий является технология обеспечения целостности БНД, которая позволит полностью или частично реализовать свойства актуальности, системности, непротиворечивости, адаптивности, комплексности и доступности.

1.2 Анализ основных подходов к обеспечению целостности данных и информации

Как показано в подразделе 1.1, внешние и внутренние НД являются важной частью системы управления предприятием. В то же время они являются

одним из подмножеств множества документов, циркулирующих на предприятии. Поэтому для разработки и эксплуатации унифицированных технологий и систем управления в настоящее время все виды документов и данных, используемых для управления предприятием, предлагается описывать общим термином «Информационный ресурс» (ИР). Однако это понятие является многозначным, а его определение зависит от предметной области. Так, в информационных системах (ИС) управления предприятием ресурс – это использующиеся в ИС средства, привлекаемые для обработки информации [21]. ИР в ИС могут быть представлены двумя основными способами: в виде данных и в виде документов. При этом основное внимание в ИС уделяется фактографическим документам, которые отражают в системе события, происходящие в жизни предприятия [22]. Поэтому большинство описаний ИР ИС и операций над этими ресурсами основаны на ограниченном количестве базовых формальных моделей.

ИР ИС предприятия должны соответствовать ряду требований, среди которых одно из ключевых – безопасность. Согласно [23] безопасность информации (данных) – это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Рассмотренное определение термина «безопасность информации (данных)» базируется, в свою очередь, на ряде терминов, определения которых приведены в соответствии с [24-27]:

– информация – это сведения (сообщения, данные) независимо от формы их представления;

– данные (Д) – это факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации;

– информационная система (ИС) – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

– документ – это значимые данные, представленные на соответствующем носителе;

– конфиденциальность информации – это состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

– доступность информации – это состояние ресурсов информационной системы, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

– целостность информации (ЦИ) – это состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

– угроза (безопасности информации) – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Анализ приведенных определений позволяет сделать вывод о том, что наряду с конфиденциальностью и доступностью, ЦИ (данных) – одно из

обязательных условий существования безопасности информации - представлено на рисунке 1.2. ЦИ (данных) определяет сохранность качества информации и ее свойств (полнота, точность, последовательность) на протяжении всего жизненного цикла.

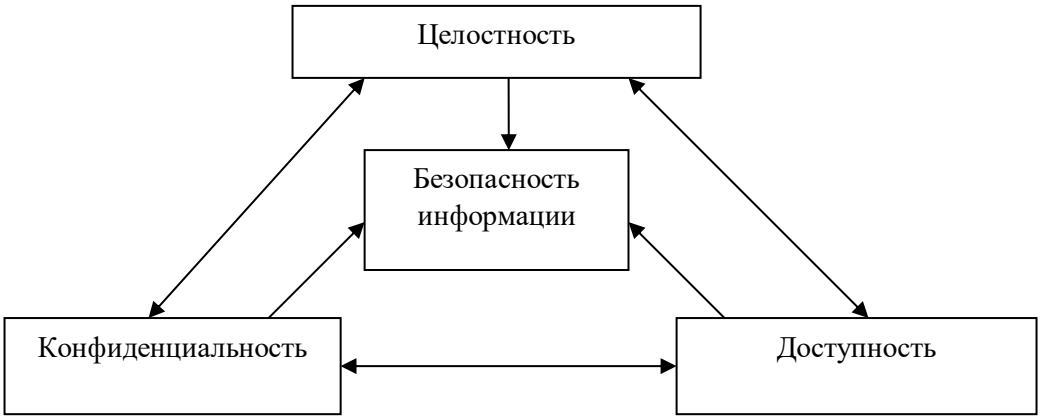

Рисунок 1.2 – Целостность, конфиденциальность и доступность как условия существования безопасности информации

Организация обеспечения ЦИ как и информационной безопасности (ИБ) в целом, основывается на анализе угроз ее нарушения - представлено на рисунке 1.3.

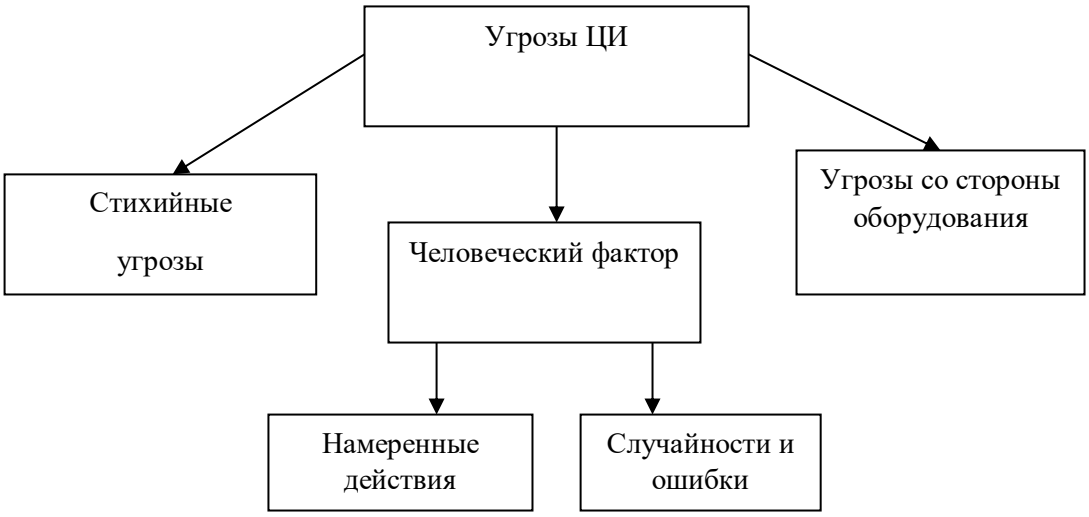

Рисунок 1.3 – Источники угроз нарушения целостности информации (данных)

Угроза обладает способностью наносить ущерб, который может возникать из-за атаки на информацию, на саму систему или иные ресурсы, приводя, к их разрушению, раскрытию, модификации, порче, недоступности или потере [27, с. 2-20].

Суть угроз по их видам раскрывается согласно [28-35]. Стихийные угрозы связаны с плохо прогнозируемым воздействием факторов среды (землетрясения, наводнения, пожары, ураганы, молнии, аварии и другие форс-мажорные обстоятельства), которые могут физически повредить элементам ИС предприятия, либо помешать их стабильной работе.

ЦИ может также быть нарушена из-за полного выхода из строя либо временных сбоев в работе оборудования (средств связи, аппаратуры, систем жизнеобеспечения и питания) или некорректно работающего программного обеспечения.

Кроме того, на состояние информации оказывает влияние человеческий фактор, который в свою очередь разделяется на намеренное и неумышленное воздействие.

ЦИ представляют угрозу намеренные действия (саботаж, уничтожение, хищение, перехват, модификация информации, внедрение вредоносных программ и т.д.) сторонних злоумышленников, и лиц, имеющих доступ к внутренней информации предприятия, в том числе его недобросовестных сотрудников. Наиболее распространенной угрозой ЦИ является ее намеренное уничтожение, либо модификация в результате несанкционированного доступа (НСД) пользователя к ИР ИС.

Также нарушить ЦИ (данных) могут неумышленные действия пользователей ИС (халатность, ошибки на этапе проектирования, ошибки из-за недостаточной квалификации персонала, случайное удаление файлов, ошибки маршрутизации, иные ошибки и несчастные случаи) при обработке, хранении или транспортировке информации.

Угрозы ИС могут оказывать активное воздействие (физически повреждать элементы ИС или нарушать данные и их внутреннюю структуру), либо пассивное (например, несанкционированное копирование информации) [35, с. 347-350].

В результате анализа угроз ИС, а также ее собственных уязвимых мест, вырабатывается комплекс разнородных защитных мер направленных на сохранение ИБ и ЦИ.

Государство со своей стороны обеспечивает законодательную правовую основу защиты информации, ведется разработка нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением [23, с. 2-11; 31, с. 350-353]. Предприятие на своем уровне также утверждает и применяет НД направленные на контроль и защиту ИС, в рамках политики безопасности компании.

Для физической защиты элементов ИС проводятся организационные мероприятия, обеспечивающие защиту территорий, зданий, помещений, оборудования, на котором располагаются ИР и носителей информации. Такие меры и средства защищают от воздействия природных факторов и создают препятствия для проникновения неуполномоченных лиц к объекту защиты. Разрабатываются и применяются специальные меры по хранению информации

и ее носителей, доступу к ней (различные охранные и пропускные режимы, правила пользования документами, их транспортировки, уничтожения).

Для защиты ЦИ от сбоев и отказов оборудования и программного обеспечения принимаются меры связанные с проверкой и тестированием на всех этапах его эксплуатации (приобретение, введение в строй, функционирование, вывод из эксплуатации), профилактические мероприятия для поддерживания работоспособности [36], строгий контроль внесения изменений.

Для защиты информации от намеренного или непреднамеренного воздействия и ошибок со стороны персонала проводится разносторонняя работа с кадровым составом (инструктаж, обучение, мотивация, контроль) на этапах подбора соответствующих сотрудников, предоставления им прав доступа к ИС и ее ресурсам, дальнейшей работе, увольнении [31, с. 350-353].

Специфической областью является организация защиты целостности данных, содержащихся в электронном виде в памяти ЭВМ. В данном случае наряду с организационными, применяются также программно-технические меры защиты информации.

Осуществляется резервное копирование (периодичность создания зависит от важности информации) с проверкой сохранности ЦИ. Резервные копии БД и иной информации необходимы для их восстановления в случае нарушения ЦИ [37, 38]. Эффективная стратегия восстановления основана на размещении данных на нескольких уровнях хранения. Такими уровнями могут выступать:

– высокоскоростное онлайн хранилище (хранятся актуальные данные и копии последних версий для быстрого восстановления);

– низкоскоростное онлайн хранилище (хранятся более старые копии данных, используются реже);

– автономное хранилище (удаленно расположенное хранилище, объем зависит от носителя, не используется для повседневного восстановления, может храниться информация за все время деятельности предприятия);

– хранилище объектов (управляет данными представленными в виде объектов, обеспечивает доступность объектов с учетом их версий и истории изменений).

Каждый из уровней хранения копий важен, какими из них воспользоваться, компания выбирает в зависимости от сценария повреждения и восстановления данных.

Для защиты информации от НСД пользователь должен пройти определенные этапы проверки, перед тем как получить право на работу с тем или иным видом информации. Прежде всего, имеется в виду взаимосвязанные процессы идентификации и аутентификации [35, с. 347-350; 39, 40].

Идентификация – это процесс присвоения пользователю уникального идентификатора и проверка его по списку присвоенных идентификаторов.

Идентификатор – это уникальная информация об объекте, по которой он отличается от других объектов (имя, логин, номер).

Аутентификация – это проверка принадлежности пользователю предъявленного идентификатора, подтверждение подлинности (удостоверение, пароль, биометрические данные).

Для доступа к информации система защиты должна найти в списке предъявленный идентификатор и проверить его принадлежность данному пользователю.

После идентификации и аутентификации пользователя должен быть определен уровень его доступа к использованию ИР ИС. Управление доступом – способ защиты ИС путем регулирования использования ИР [35, с. 347-350]. Методы разграничения доступа делят на:

– списочный (для каждого пользователя составляется список ресурсов и прав доступа к ним, для каждого ресурса – список пользователей и их полномочий);

– матричный (задается особая таблица полномочий, где строками являются идентификаторы субъектов, столбцами – ИР, а каждый элемент содержит перечень полномочий по работе данного субъекта с данным ресурсом);

– по категориям и уровню секретности (пользователь имеет право работать со всеми ресурсами, чей уровень секретности или категория важности не выше уровня допуска субъекта).

Перечисленные методы разграничения доступа к ИР ИС при необходимости могут быть усилены парольной системой защиты.

Также различают дискретизационный и мандатный принципы управления доступом к информации [35, с. 347-350; 41].

При реализации дискретизационного принципа контроля доступа система контролирует доступ именованных субъектов (пользователей) к именованным объектам (файлам, программам). Для каждой пары (субъект - объект) задается исчерпывающее перечисление допустимых типов операций (чтение, запись), которые субъект имеет право производить над объектом. Механизм, предусматривает санкционированное изменение правил разграничения доступа, в том числе списка пользователей и объектов.

При реализации мандатного принципа контроля доступа каждому субъекту и каждому объекту присваивают классификационные метки, отражающие их место в соответствующей иерархии [41, с. 2-7]. При работе система запрашивает и получает от пользователя соответствующие метки. При санкционированном внесении в список пользователей нового субъекта ему должны быть назначены новые метки.

Субъект может читать объект, если его уровень в иерархической классификации не меньше, чем уровень субъекта. Субъект осуществляет запись в объект, если его уровень в иерархической классификации не больше, чем уровень объекта.

Реализация мандатного принципа контроля доступа предусматривает возможность изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

Еще одним подходом к защите данных и контролю их целостности является применение криптографических методов. Шифрование – это процесс преобразования данных с использованием набора ключей или секретных данных [33, с. 102; 37, с. 226; 42]. Только тот, кто владеет ключами, может совершить обратное преобразование данных в пригодный для использования формат. Вид шифрования зависит от природы данных, степени их важности и конфиденциальности.

Выделяют два основных метода шифрования данных [40, с. 36; 42, с. 71]:

– симметричное шифрование (для зашифровки и расшифровки используется один и тот же секретный ключ);

– асимметричное шифрование (один ключ используется для зашифровки, другой для расшифровки, причем один из ключей открытый, другой секретный).

На практике эти методы часто сочетают из-за низкого быстродействия асимметричного шифрования при работе со сложными задачами.

Также различают три уровня шифрования данных [42, с. 337]:

– при транспортировке данных по сети (используется специальный криптографический протокол Secure Sockets Layer (SSL) актуальной версии и виртуальная частная сеть Virtual Private Network (VPN), а также защищенный сервис управления ключами);

– при хранении данных в БД (методы маскировки, добавление фиктивных данных при каждой вставке, пакетная вставка для недопущения отслеживания атомарных вставок);

– при хранении данных в файловой системе (применяется шифрование данных перед помещением в файловую систему, шифрование на уровне самой файловой системы и на уровне устройств).

Важным понятием в обеспечении ЦИ криптографическими методами является электронная цифровая подпись (ЭЦП). ЭЦП – это особая совокупность информации, прикрепляемая к документу (или другой информации) и применяемая для аутентификации лица подписавшего документ [43, 44]. По сути ЭЦП – реквизит, позволяющий проверить наличие искажений в документе с момента прикрепления подписи и принадлежность подписи владельцу сертификата.

ЭЦП – результат криптографического преобразования информации с использованием ключа. Применение ЭЦП позволяет обеспечить:

– контроль целостности подписанного ЭЦП документа и выявление подделок (при модификации содержания подпись станет недействительной, так как она прямо связана с исходным состоянием документа);

– подтверждение авторства и невозможность отказа от него (так как закрытый ключ известен только владельцу ЭЦП, он может доказать свое авторство и не может отказаться от него).

Схема ЭЦП состоит из трех этапов [44, с. 3]:

– генерация пары ключей (на основе выбора закрытого ключа вычисляется соответствующий открытый);

– формирование подписи (для конкретного документа вычисляется ЭЦП на основании закрытого ключа);

– верификация (для конкретных документа и подписи при помощи открытого ключа определяется действительность ЭЦП).

ЭЦП может формироваться на основе симметричного и асимметричного методов шифрования. Последний более распространен в современных условиях, причем собственно подписание происходит с применением закрытого ключа, а расшифровка – с применением открытого [43, с. 8].

В процессах формирования и проверки ЭЦП может применяться механизм хэш-функций.

Хэш-функция – это функция, преобразовывающая строки бит произвольной длины в строки бит фиксированной длины [42, с. 264; 45]. Результатом хэш-функции является хэш-код – строка бит определенной длины. По сути, при помощи хэш-функции можно сжать конкретный документ или сообщение в строку длиной несколько десятков (сотен) бит.

Формируя ЭЦП, отправитель вычисляет хэш-функцию набора данных (документа), который подписывается и получает его хэш-код. Затем применяется шифрование секретным ключом отправителя, и получаемая цифровая последовательность считается ЭЦП данного документа. Для проверки ЭЦП получатель снова вычисляет хэш-функцию данного документа, после чего при помощи открытого ключа сверяет соответствие фактического значения вычисленному.

Хэш-функции также могут служить для контроля ЦИ. Для каждого документа (сообщения) вычисляется хэш-код, который передается вместе с данными. При получении данных вычисляют значение хэш-функции и сравнивают его с контрольным значением. Если значения не совпадают, данные были модифицированы.

Криптографические хэш-функции должны обладать следующими тремя свойствами [42, с. 265; 45, с. 7]:

– невозможность восстановить исходное сообщение по данному значению хэш-функции;

– невозможность найти два сообщения с одним и тем же значением хэш-функции;

– невозможность по данному сообщению найти другое сообщение с тем же значением хэш-функции.

Существуют также специальные подходы к обеспечению ЦИ, основывающиеся на т.н. моделях контроля целостности данных Кларка-Вилсона и Кена Биба.

Дискреционная модель Кларка-Вилсона основывается взаимосвязи «субъект – операция (транзакция) – объект», причем операция не должна нарушать целостности объекта [34, с. 60; 35, с. 348; 40, с. 81; 46]. Модель имеет несколько основных положений:

– все множество объектов (данных ИС) M делится на подмножество объектов A, целостность которых подтверждена (контролируется) и

подмножество объектов B проверка целостности которых не проведена, A и B не пересекаются;

– среди операций над объектами выделяются процедуры преобразования P, которые переводят систему из одного состояния в другое;

– вводится особый класс процедур V, которые обеспечивают проверку целостности контролируемых данных;

– если результат процедуры преобразования P проходит проверку целостности V, то транзакция считается корректной.

В соответствии с моделью устанавливаются следующие правила:

1. Множество процедур контроля V должно содержать процедуры контроля целостности любого элемента данных из A.

2. Все процедуры преобразования P должны быть корректными транзакциями, а их применение к A, сохранять целостность.

3. Допустимость применения P к элементам A должна контролироваться системой и только P могут изменять A.

4. Список разрешенных конкретным пользователям процедур P с указанием допустимого для каждой P и данного пользователя набора обрабатываемых элементов A ограничен.

5. Функциональные обязанности субъектов должны быть разграничены, т.е. субъект не может изменять A без вовлечения в операцию других субъектов (принцип совместного выполнения).

6. Специальные P могут корректно обрабатывать B, превращая их в A.

7. Каждая P должна записывать информацию достаточную для восстановления всей картины применения этой P в особый элемент A (журнал регистрации). Журнал регистрации предназначен только для добавления в него информации.

8. Система должна аутентифицировать всех пользователей, пытающихся выполнить какую-либо процедуру преобразования P.

9. Только специально уполномоченный пользователь (субъект) может изменять списки, определенные в правилах б) и г).

ЦИ в мандатной модели Кена Биба достигается запретом движения «опасных» потоков «снизу вверх», чтобы они не нарушили целостность объектов более высокого уровня [34, с. 61; 35, с. 349; 40, с. 80; 46, с. 146].

В общем виде правила сохранения целостности в модели Биба сформулированы так:

– субъект не может читать информацию более низкого уровня целостности (No Read Down);

– субъект не может записывать информацию на более высокий уровень целостности (No Write Up).

Эти правила для субъекта находящегося на условном среднем уровне ЦИ схематически представлены на рисунке 1.4.

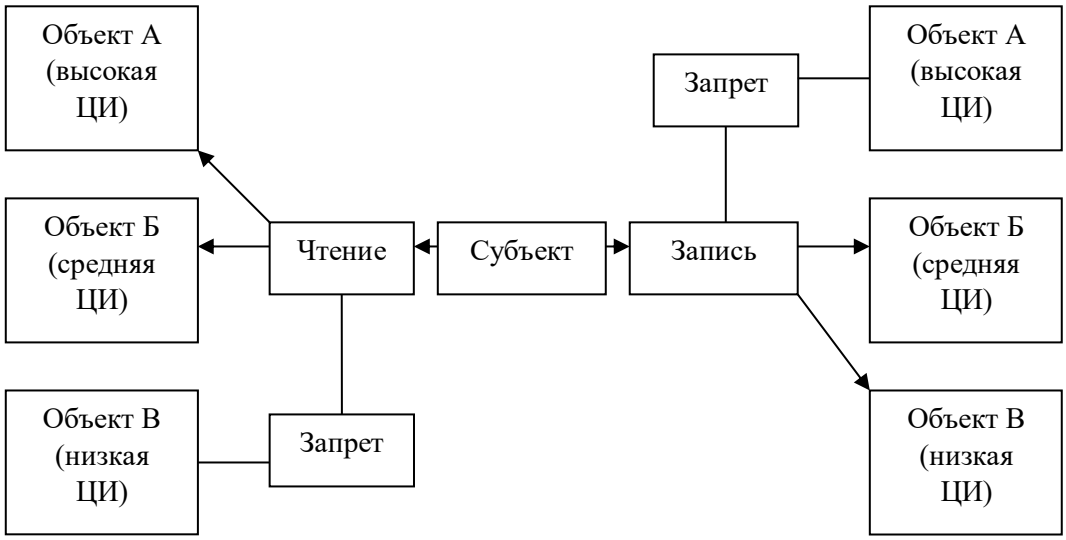

Рисунок 1.4 – Правила сохранения целостности в модели Кена Биба

В отдельных случаях субъекту может быть разрешено чтение из объекта с более низкой ЦИ, но тогда уровень целостности самого субъекта понижается до уровня объекта. Также в отдельных случаях возможна запись вверх, но тогда уровень объекта с более высокой ЦИ понизится до уровня записывающего субъекта [40, с. 35].

В различных источниках приводятся разные определения целостности, например, по [28, с. 8] целостность данных используется для описания точности и корректности хранящейся в базе информации, с учетом того что система управления базами данных (СУБД) обеспечивает декларативную поддержку и выполнение установленных ограничений. Ограничением в данном случае считается правило БД, которое не допускает попадания в базу ошибочных, либо некорректных данных.

При этом БД должна обеспечивать как обработку запросов в системах с одним пользователем, так и одновременный доступ множества пользователей, и соответственно обработку множества запросов к информационным объектам. В таком случае для обеспечения ЦИ (данных) в понимании правильности и непротиворечивости содержимого БД, служит управление транзакциями.

Под транзакцией, согласно [38, с. 20; 47], понимается упорядоченная и неделимая с точки зрения воздействия на БД последовательность операторов обработки данных (чтения, вставки, удаления модификации), при которой: а) либо результаты всех операторов входящих в транзакцию, отображаются в БД и переводят ее из одного состояния в другое; б) либо воздействие этих операторов отсутствует.

Успешная транзакция переводит БД из одного согласованного состояния в другое, при этом под согласованностью понимается выполнение всех ограничений целостности [48]. В ходе выполнения транзакции возможно

временное нарушение согласованности, но с окончанием транзакции, оно должно быть восстановлено.

Транзакции обладают определенными свойствами [49-51]:

– атомарность (транзакция неделима, выполняется либо вся транзакция целиком, либо ни одна из ее частей);

– согласованность (транзакция начинается при согласованности данных и заканчивается, оставляя данные согласованными);

– изоляция (одни транзакции не должны создавать помехи выполнению других транзакций);

– долговечность (изменения принятые в результате транзакции не должны быть утеряны, только другая транзакция может вернуть исходное состояние системе).

Все основные СУБД, включая MS Access, Oracle, SQL Server и DB2, поддерживают управление транзакциями [48, с. 120].

Для управления транзакциями в системах, поддерживающих язык Structured Query Language (SQL) используются следующие основные операторы:

1. COMMIT для фиксации результата транзакции и запоминания изменений.
2. ROLLBACK для отката транзакции и отмены изменений.

Если операторы, объединенные в транзакцию, успешно выполнены, то происходит нормальное завершение транзакции и БД переходит в новое целостное состояние (COMMIT). Если же на этапе выполнения транзакции происходит сбой, то применяется откат к исходному состоянию (ROLLBACK) [47, с. 148].

СУБД отслеживает все транзакции, которые вносят изменения в БД при помощи журнала транзакций. Журнал транзакций – это часть БД в которую поступают сведения обо всех изменениях всех объектов [38, с. 89]. Ведение такого журнала обеспечивает возможность восстановления целостного состояния БД после сбоев, поэтому в некоторых системах файл журнала транзакций следует хранить на разных дисках.

Параллельная работа с БД множества пользователей может привести к проблемам в функционировании системы (потеря изменений, считывание результатов незавершенных транзакций, игнорирование корректных изменений и т.д.) и нарушению ЦИ [48, с. 184; 49, с. 272; 50, с. 29; 51, с. 48].

Для избегания и решения подобных проблем важно различать уровни изоляции транзакций. Чем выше уровень изоляции конкретной транзакции, тем меньше вероятность, появления помех со стороны других параллельных транзакций. Самым высоким уровнем изоляции считается сериализуемый. При применении сериализации транзакций результат совместного выполнения транзакций эквивалентен результату их выполнения в некоторой последовательности [47, с. 3-250].

В реляционных БД аспект целостности также связан с двумя базовыми требованиями: должны быть обеспечены целостность сущности и ссылочная целостность.

Целостность сущности обеспечена, если любой кортеж отношения отличим от другого кортежа данного отношения по первичному ключу, то есть каждая строка в таблице имеет свой идентификатор [48, с. 40; 50, с. 50]. Таким образом, уникальный первичный ключ должен идентифицировать каждую сущность и в составе этого ключа не должно быть неопределенных значений.

Ссылочная целостность обеспечена, если внешний ключ (первичный ключ одной таблицы, который был помещен в другую для создания общего атрибута) дочернего отношения содержит некое значение, то это же значение должно присутствовать в первичном ключе родительского отношения [48, с. 42; 51, с. 72; 52]. Другими словами, каждое значение внешнего ключа должно быть либо NULL, либо действительным значением в первичном ключе связанной таблицы.

Таким образом, ЦИ (данных) должна быть обеспечена с учетом соответствующих реакций на возможные угрозы. Чтобы обеспечить комплекс таких реакций, необходим системный подход к защите информации, который включает правовые, организационно-административные, программно-технические и другие меры противодействия угрозам.

Однако существующие подходы к решению такой важной проблемы, как целостность ИР ИС управления предприятием, в настоящее время кардинально различаются. В части проанализированных подходов как в [53] задача обеспечения целостности представляет собой задачу обеспечения правильности данных в базе данных (БД) (в максимально возможной степени). Декларативными решениями этой задачи являются предикаты, описывающие ограничения целостности и дающие при проверке значения «TRUE».

В другой части подходов под целостностью ресурсов ИС понимается состояние, при котором их изменение осуществляется преднамеренно субъектами, имеющими на него право. При этом сохраняются состав, содержание и организация взаимодействия ресурсов ИС [21, с. 6].

В результате такого расхождения остаются открытыми вопросы обеспечения правильности состава, содержания и организации взаимодействия ИР различной природы. В частности, уникальных решений требует организация проверки правильности состава, содержания и организации взаимодействия различных документов, а также документов и БД ИС. Поэтому проведение исследований, направленных на разработку новых и модификацию существующих решений по унификации обеспечения целостности ИР ИС следует считать актуальным.

1.3 Анализ теоретических исследований и прикладных работ по обеспечению целостности информации

1.3.1 Обзорный анализ теоретических исследований в области обеспечения целостности информации

Спектр угроз безопасности и целостности информации (данных) в настоящее время достаточно широк, что требует постоянного развития специальных технологий защиты и поддержания ИБ и ЦИ. Изучению этой проблемы посвящено ряд публикаций, в которых анализируются существующие подходы и предлагаются новации в данной сфере.

В последние годы исследования, посвященные решению проблемы обеспечения целостности документов как ИР ИС, можно разделить на два основных направления. Первое из них посвящено исследованию подходов, моделей, методов и способов решения этой проблемы, которые не привязаны к особенностям конкретной предметной области.

Так в [54] рассматриваются основные угрозы целостности информации, а также методы ее защиты на этапах хранения и передачи. В частности описан механизм резервного копирования с использованием отказоустойчивых носителей на этапе хранения информации. Кроме того, на этапе передачи данных для контроля их целостности проанализированы методы контроля ЦИ основанные на криптографических преобразованиях (использование ЭЦП, хэш-функций, кодов проверки подлинности).

В работе [55] предложен метод обеспечения ЦИ с минимизацией избыточности, которая возникает при последовательном применении криптографических методов и резервного копирования, а также одновременной локализацией данных, целостность которых нарушена. В [56] минимизация избыточности дополняется использованием правил построения помехоустойчивых кодов и возможностью контроля целостности эталонных хэш-кодов, а не только защищаемых данных.

Предлагаемая в [57] методика позволяет обеспечить ЦИ с учетом принятых ограничений, при помощи расчета рациональных параметров резервирования информации для ее оперативного восстановления, рассчитанных на основе требуемой вероятности обеспечения ЦИ.

Однако резервное копирование данных с дальнейшим их хранением, которое является основой вышеперечисленных [54, с. 123; 55, с. 52; 56, с. 53; 57, с. 214] методов и подходов подразумевает, что информация будет оставаться неизменной определенное, иногда длительное время. Это не всегда возможно в силу объективных причин, например, изменение законодательных норм, стандартов, особенностей бизнес-процессов. Важно учитывать, что некоторые изменения повлекут за собой значительную корректировку информации и необходимость ее повторного резервирования. Криптографические методы в данных работах выполняют функции аутентификации, установления авторства и защиты от подделок и взлома, но полностью не решают проблемы обеспечения целостности состава и содержания документов.

В [58] рассматривается архитектура системы, которая может проверить целостность платформы электронных документов на основе блокчейна с применением метода предварительной проверки электронных документов. Однако в [58, p. 57] практически не рассматриваются ситуации изменений в массиве документов, вызванных совершенствованием юридической базы бизнеса или сценариев осуществления бизнес-процессов. Причиной этого является трактовка в [58, p. 60] понятия целостности ресурсов ИС только с позиций изложенных в [21, с. 6]. Поэтому цель исследования [58, p. 54] ограничена разработкой способов доказательства стабильности электронных документов в блокчейн-платформе.

Отдельно в рамках этого направления рассматриваются вопросы разработки и совершенствования методов проверки электронных и печатных документов. В [59] предлагается метод проверки документов, предназначенный для обеспечения аутентичности, целостности, доступности и предотвращения отказа от авторства. Однако основной целью применения этого метода является предотвращение фальсификации документов. Отдельно задача обеспечения целостности документов как разновидности ИР ИС в [59, p. 625] не рассматривается.

Для обеспечения целостности и подлинности информации содержащейся в документе в [60] предлагается механизм формирования электронной версии документа (для переноса на бумажный носитель и подписания клиентом) и последующей проверки бумажной версии документа организацией с применением уникального идентификатора, формированием ЭЦП и внесением ЭЦП в документ в формате QR-кода.

Разработанный в [61] метод позволяет генерировать идентификаторы авторов на основе содержимого документа и биометрических характеристик подписи субъекта. Для подтверждения целостности и аутентичности документов на основе подписи формируется скрытый биометрический идентификатор, который встраивается в текстовые документы на электронных и бумажных носителях. Таким образом, выполняются сразу две задачи: защита документа от подделок и проверка его авторства.

Еще один подход к обеспечению подлинности и неизменности документа (представленного в бумажном либо электронном виде) предложен в [62]. Для защиты документа (как физического, так и электронного) предлагается способ формирования водяного знака (расстановка «специального шума», цветовая модификация определенных пикселей), который может применяться как для проверки подлинности, так и для скрытой передачи информации.

В [63] рассматривается аутентификация электронных и аналоговых документов в процессе документооборота с учетом отличий и этапов их жизненных циклов. При взаимодействии разных ИС для контроля целостности отмечается целесообразность применения усиленной электронной подписи (с использованием средств криптографической защиты). При этом возникает необходимость в специальных методах и технологических решениях для

контроля аутентичности и целостности документов после истечения срока действия сертификатов ключей ЭЦП.

Поход к организации многофакторной аутентификации пользователей информационных систем предложен в [64]. Используются методы динамической биометрической аутентификации на основе динамики рукописного почерка. Предложен комплекс технических средств для получения биометрический данных пользователя, процедуры их анализа и алгоритм доступа к ИР (с использованием дискретного преобразования Фурье и системы ортогональных функций Хаара). Акцент в данном методе сделан на подтверждении личности, вступающей в информационный обмен.

В [65] ЦИ рассматривается как составляющая ИБ в базах данных корпоративных информационных систем. На примере SQL Server описаны механизмы обеспечения целостности данных современных СУБД (в том числе сущностная, доменная и ссылочная целостность).

Подход к контролю целостности данных в сфере облачных вычислений (облачный аудит) предложен в [66]. Основой подхода является вариация гомоморфной криптографической системы Пэйе с гомоморфной меткой и комбинаторными пакетными кодами. Также предлагаемый метод поддерживает динамические операции с данными с меньшими вычислительными затратами и лучшей защитой от влияния человеческого фактора (атаки, подлог, порча и неправомерное использование данных).

Второе направление посвящено исследованию частных случаев решения проблемы обеспечения целостности документов как ИР конкретных ИС или же ИС для конкретной предметной области. Однако в большинстве публикаций предлагаемые решения рассматривают применение уже известных методов и способов обеспечения целостности документов различного назначения. Так, в [67] рассмотрено решение задачи обеспечения целостности журнала аудита действий пользователя в приложении Skyline. Это приложение предназначено для создания целевых методов масс-спектрометрии и количественного анализа данных. Для защиты целостности журнала аудита в [67, p. 4367] рекомендуется применение встроенных хэшей. Решение задачи обеспечения целостности состава и содержания журнала аудита действий в [67, p. 4368.] не рассмотрено.

В [68] представлено описание платформы SPROOF, предназначенной для децентрализованной обработки и управления цифровыми документами в сфере образования. Однако и в этом случае решение задачи обеспечения целостности документов основано на использовании хэшей и механизма ключей. Решение проблемы обеспечения целостности состава и содержания документов с учетом их возможных изменений с течением времени в [68, p. 18] не приведено. Причиной этого является исходное предположение о неизменности состава и содержания цифровых документов, на котором базируются приведенные в [68, p. 23] результаты.

Механизм ключей является основой решения задачи обеспечения целостности в системе биометрических электронных идентификационных документов, архитектура которой предлагается в [69]. Кроме того, для

проверки аутентификации пользователя в [69, p. 10-1-10-13] предлагается использовать биометрическую систему электронного удостоверения личности. Однако материалы исследования [69, p. 10-10-10-17] основаны на предположении, что все документы на протяжении длительного времени остаются неизменными. Такое предположение может быть справедливым для тех предметных областей, в которых состав и содержание документов как ИР не меняется на протяжении длительного времени. Примером такой предметной области могут служить рассмотренные в [70] безналичные финансовые транзакции. Поэтому одним из ключевых компонентов таких транзакций в [70, p. 87] считается целостность данных, а не целостность документов. Возможность изменения состава банковских транзакций в [70, p. 88] не рассматривается.

Модель мандатного контроля ЦИ (данных) для микроядерной операционной системы KasperskyOS представлена в [71]. При выполнении необходимых для работы модели требований, не возникают информационные потоки от менее целостных компонентов системы к более целостным, либо компонентам с несравнимым уровнем целостности, возможны только разрешенные информационные потоки. В случае захвата части системы с определенным уровнем целостности компонентов не происходит компрометации части системы с более высокими или несравнимыми уровнями целостности.

Наибольшее внимание в современных исследованиях уделяется вопросам обеспечения целостности документов в различных e-health ИС. При этом основное внимание сейчас уделяется проблемам, связанным с заполнением, хранением и обработкой электронных медицинских карт пользователей. Однако и в этом случае основное внимание в ходе решения проблемы обеспечения целостности ИР уделяется вопросам аутентификации источников документов и обеспечению защиты документов от взлома. Так, в [72] для обеспечения целостности электронных медицинских карт в облачной среде предлагается проверяемая схема шифрования подписей на основе атрибутов с помощью блокчейна. Также, в [72, p. 170722] предлагается хранить каждую операцию с электронной медицинской картой как транзакцию в общедоступной цепочке блоков, что гарантирует невозможность изменения таких карт. Однако в [72, p. 170713-170730] не рассматривается возможность изменения состава и содержания электронной медицинской карты из-за появления новых методов и средств диагностики.

В [73] предлагается решение задачи обеспечения целостности для централизованного хранилища электронных медицинских карт. Однако предлагаемое в [73, p. 311] решение основано на двусторонней аутентификации для авторизованных пользователей, проверке подписи входящего запроса и уведомлении системы об угрозах. Вопросы обеспечения целостности состава и содержания электронной медицинской карты в результате вносимых в нее изменений и дополнений остаются в [73, p. 312] нерешенными.

Проведенный анализ публикаций позволяет утверждать, что современные варианты решений проблемы обеспечения целостности ИР обладают такими особенностями:

– они направлены, главным образом, на решение задач аутентификации источников документов и защиты документов от несанкционированного взлома;

– они основаны на предположениях о стабильности массива документов в эксплуатируемых ИС и о неизменности состава и содержания документов в ходе эксплуатации ИС на протяжении длительного времени;

– вопросы правильности содержания документов в ИС решаются исключительно на уровне БД, в которых организовано хранение фактографических данных из документов различного рода.

Вопросы обеспечения целостности ИР ИС, автоматизирующих изменяющиеся во времени процессы предприятия, следует признать решенными лишь частично. Основной нерешенной частью проблемы обеспечения целостности следует признать отсутствие моделей и методов, позволяющих обеспечить правильность состава и содержания документов как источников входной, промежуточной и выходной информации ИС. Все это дает основания утверждать, что целесообразным является проведение исследования, посвященного совершенствованию модели целостности ИР системы управления предприятием (СУП).

1.3.2 Обзорный анализ прикладных решений по обеспечению целостности информации и документов

Сегодня на рынке услуг по ведению документации предприятия представлен ряд прикладных программных продуктов, которые решают вопросы обеспечения безопасности и целостности информации, в том числе – обеспечения целостности документов и, в частности, обеспечения целостности НД предприятия.

«1С: Предприятие» представляет собой комплексное прикладное решение, позволяющее организовать ИС, обеспечивающую финансово-хозяйственную деятельность предприятия [74].

В рамках программного продукта «1С: Предприятие» вопросы безопасности и целостности информации (данных) решаются за счет применения нескольких механизмов контроля.

При подключении к базе данных через веб-сервер используется многоуровневая аутентификация. Первый уровень обеспечивается средствами самого веб-сервера в момент соединения, при этом пользователь использует вид аутентификации, который поддерживается его браузером. Второй уровень аутентификации выполняется средствами самого «1С: Предприятия» при установке соединения с информационной базой [22, с. 247; 75].

В случае аутентификации средствами «1С: Предприятия» пользователь при начале работы указывает имя и соответствующий этому имени пароль, в случае аутентификации средствами операционной системы происходит анализ,

от имени какого пользователя выполняется подключение, и на этом основании определяется конкретный пользователь.

Для защиты передаваемой информации от НСД в «1С: Предприятие» служит шифрование данных с применением различных алгоритмов. Для защиты канала передачи данных между веб-клиентом и веб-сервером используются криптографические протоколы SSL или TLS, поддержку этих протоколов обеспечивает HTTPS соединение. Для защиты каналов передачи данных между кластером серверов и клиентами, а также для защиты каналов внутри самого кластера используются алгоритмы шифрования данных, реализуемые системой «1С: Предприятие»: RSA и Triple DES. Защита канала передачи данных между кластером серверов и СУБД осуществляется средствами той СУБД, которая используется [22, с. 73].

Также система «1С: Предприятие» позволяет описать наборы прав доступа и работы с данными, соответствующие должностям пользователей или видам их деятельности (ролям). В этом случае над конкретным объектом, хранимым в БД возможно действие (чтение, добавление, изменение, удаление) только если ограничение доступа для данных этого объекта принимает значение «Истина» [22, с. 160; 75, с. 183].

Кроме того, для дополнительного контроля, события, происходящие в информационной базе, а также история работы пользователей фиксируются в журнале регистрации [75, с. 146], осуществляется резервное копирование информационной базы [76].

Система «1С: Предприятие» для повышения производительности и одновременного обеспечения целостности данных поддерживает уровни изоляции транзакций вплоть до сериализуемого, который полностью изолирует транзакции друг от друга и минимизирует ошибки и сбои.

Также для «1С: Предприятие» представлена отдельная утилита контроля целостности, которая осуществляет мониторинг состояния объектов файловой системы и базы данных и фиксирует изменения этих объектов. Неизменность объектов контролируется путем сравнения хэш-сумм, которые вычислены по алгоритму SHA-1. Процесс проверки состоит из формирования эталонных значений хэш-сумм и последующей регулярной сверки [77].

Наряду с «1С: Предприятие» свои решения в виде Enterprise Resource Planning (ERP) продуктов предлагает компания SAP AG. Из линейки продуктов самым популярным считается mySAP ERP, который является эволюционным продолжением SAP R/3 [78].

Технология всех решений mySAP основывается на многоуровневой архитектуре клиент/сервер [79]. Трехуровневая технология клиент/сервер включает: уровень презентации (пользовательский уровень), уровень приложения и уровень базы данных. Все три уровня могут быть реализованы на одном компьютере, либо на разных.

Целостность и безопасность данных обеспечивается за счет системы проверки полномочий каждого пользователя, с допуском к данным только лиц имеющих на это право [79, с. 347]. Для этого предусмотрен специальный

механизм Central User Administration (CUA) с помощью которого можно унифицировать учетные записи, назначать права и полномочия пользователям, управлять свойствами учетных записей.

Концепция пользователя SAP лежит в основе метода обеспечения безопасности данных и транзакций. Данные о пользователе хранятся и обновляются в основных записях по пользователю, а безопасность обеспечивается соответствующими профилями и авторизациями [80]. При этом авторизованному пользователю может быть позволен как полный доступ к системе, так и ограниченный узким перечнем его функциональных обязанностей.

В качестве средств дополнительного контроля может использоваться системный журнал, фиксирующий происходящие в системе события, включая запросы пользователей на доступ к защищаемым данным, действия по их изменению и т.д., а также специальные утилиты, позволяющие выполнять резервное копирование данных для повышения надежности и возможности восстановления после сбоев [80, с. 51].

Для криптографической защиты данных компания SAP AG предоставляет специальные программные интерфейсы – Secure Network Communications (SNC) и Secure Store and Forward (SSF) [81]. С помощью SNC можно, например, защитить общедоступный канал связи. При установке соединения, стороны пройдут взаимную аутентификацию на основе ЭЦП и, при настройке соответствующего режима защиты, будет обеспечен контроль ЦИ, передаваемой по данному каналу. Электронные документы на платформе SAP NetWeaver защищаются ЭЦП, с помощью механизма SSF. К любому набору данных SSF-механизм позволяет добавлять одну или несколько цифровых подписей, а также предоставляет средства для шифрования данных для защиты их целостности.

Система электронного документооборота (СЭД) «Дело» предназначена для сопровождения всех видов документов предприятия на всех стадиях их жизненного цикла [82]. В целях поддержания безопасности и целостности данных предусмотрено использование специальных модулей, главные из которых:

– модуль поддержки ЭЦП, имеющей юридическую силу и обеспечивающий защищенный документооборот;

– использование «Мастера паролей» для авторизации пользователей в СЭД «ДЕЛО», корпоративной сети и интернете;

– модуль «КАРМА» используется для криптографической защиты информации, а также защиты данных от НСД и проникновения в систему злоумышленников.

Подписание электронной подписью и ее проверка в СЭД «ДЕЛО» реализуется через опции «ЭП и шифрование» и «Сервер удаленной проверки ЭП» [83]. Для каждого лица имеющего право подписи формируются секретный и открытый ключи, секретный используется для подписания документов и последующей дешифровки, открытый – для контроля подлинности ЭЦП. Для

проверки ЭЦП используются сертификаты, которые помещены в специальное хранилище, доступное для обращений системы при использовании криптографических операций. Возможна усиленная аутентификация с помощью eToken (USB-устройств и смарт-карт) для двухфакторной аутентификации на основе цифровых сертификатов стандарта X.509.

В СЭД «Дело» реализована поддержка платформ и технологий ведущих поставщиков решений по криптографической защите информации, таких как «КриптоПро», «Сигнал-Ком», «Аладдин Р.Д.» [84]. Шифрование сообщений, передаваемых по открытым каналам, позволяет защитить информацию от НСД.

Обеспечения безопасности данных в СЭД «Дело» реализовано с помощью Secret Disk Server NG – системы защиты корпоративных баз данных и информации на серверах от НСД, несанкционированного копирования, повреждения, кражи и т.п. [83, с. 72].

Также системы управления документооборотом как элемент систем управления содержимым в масштабе предприятия представлены решениями Enterprise Content Management (ECM) для создания единой ИС компании.

Одним из лидеров в данной сфере является продукт ELMA ECM+. Система ELMA (Elegant Management) воплощает концепцию Business Process Management (BPM), что обеспечивает адаптивность ИС к изменениям в бизнес-процессах компании [85, 86]. Также ELMA обеспечивает все функции ведения электронного документооборота предприятия.

В целях обеспечения ИБ и ЦИ предусмотрены настройки прав доступа к информации и модулям системы. Также для обеспечения сохранности данных и ограничения доступа к документу применяются криптографические методы защиты, прежде всего ЭЦП [87].

ЭЦП в ELMA ECM+ является реквизитом документа, сформированным в результате криптографического преобразования с использованием закрытого ключа, и позволяет идентифицировать автора и удостоверится в отсутствии искажений в документе. Аутентификация пользователей в ELMA осуществляется при помощи механизма логинов и паролей. Имеются возможности обеспечить вход в систему только с доверенных устройств и по электронному ключу (eToken) [88].

Еще одна ECM-система предназначенная для комплексной автоматизации документооборота предприятия это LanDocs. В качестве методов защиты информации и ее целостности в данном продукте реализована поддержка ЭЦП (подписываются и шифруются файлы, карточки документов, сообщения по документу), представлен веб-клиент с поддержкой ЭЦП и шифрования [89]. Возможно ограничение прав доступа к документам, журналам, операциям и подсистемам. По каждому документу и системным событиям ведется полная статистика для обеспечения ИБ.

Жизненный цикл каждого документа для наглядности отображен в виде дерева и списка сообщений по данному документу. Также решения, реализованные на базе LanDocs, позволяют подготовить полную отчетность по движению документов, организовывать защиту корпоративного архива [90].

Разные уровни функциональности системы представлены для различных категорий сотрудников соответственно уровням доступа. Подсистема безопасности кроме ЭЦП применяет механизмы шифрования конфиденциальных данных для защиты от НСД, а также и протоколирует действия пользователей в специальном журнале безопасности [91].

Подсистема безопасности LanDocs, реализует выпуск, хранение и отзыв сертификатов пользователей в соответствии со стандартом X.509. Также данная подсистема включает серверный и клиентский компоненты, поддерживает применение криптографических средств различных сертифицированных производителей.

В результате анализа рассмотренных прикладных решений по обеспечению безопасности и целостности информации и документов в рамках продуктов ведущих производителей, можно отметить схожесть применяемых методов защиты информации (данных). Преимущественно они реализованы в виде мер по идентификации и аутентификации пользователей, ведению журналов их действий, подтверждения авторства документов, применения криптографических преобразований информации (данных), определения прав доступа конкретных лиц к данным и функционалу систем, резервному копированию данных.

Выводы и постановка цели и задач исследования

Проведенный анализ современного состояния проблемы обеспечения ЦИ (данных) в ИС предприятия и, в частности, НД как подмножества всех документов обращающихся в компании, позволяет сделать следующие выводы.

Во-первых, в большинстве исследований обеспечение ЦИ (данных) рассматривается в рамках обеспечения ИБ ИС предприятия как необходимый элемент системы безопасности. В свою очередь, обеспечение целостности документов в качестве ИР рассматривается как часть задачи обеспечения ЦИ (данных).

Во-вторых, выделение НД как отдельного подмножества из совокупности всех обращающихся в компании документов и обеспечение их целостности, а также свойства и особенности НД объединенных в единую БНД предприятия исследованы недостаточно.

В-третьих, организация обеспечения ЦИ в рамках комплекса ИБ, основывается на анализе угроз ее нарушения и системном подходе к защите информации, который включает правовые, организационно-административные, программно-технические и другие меры противодействия угрозам.

В-четвертых, в существующих подходах к решению проблемы обеспечения целостности ИР прослеживаются расхождения. Основное внимание уделяется либо максимальному обеспечению правильности данных в БД, либо сохранению состава и содержания ресурсов, притом, что уполномоченные субъекты имеют права вносить различные изменения в ИР. Таким образом существующие модели и методы обеспечивают целостность ИР ИС либо на уровне данных, либо на уровне их авторов (источников).

В-пятых, анализ публикаций показывает, что современные методы обеспечения целостности ИР направлены, главным образом, на аутентификацию источников документов и защиты документов (в том числе нормативных) от НСД. Кроме того, в их основе лежит предположение о стабильности и неизменности состава и содержания массива документов в ходе эксплуатации ИС на протяжении определенного времени, а вопросы правильности содержания и взаимосвязей документов в ИС решаются исключительно на уровне БД.

В-шестых, рассмотренные прикладные решения по обеспечению безопасности и целостности информации и ИР применяют схожие методы защиты информации (данных). Преимущественно это идентификация и аутентификация пользователей, ведение журналов их действий, подтверждение авторства документов, криптографические преобразования информации (данных), управление правами доступа конкретных лиц к данным и функционалу систем, резервное копирование данных.

Данные выводы позволяют сделать заключение о том, что для эффективной работы БНД современного предприятия необходимы создание и реализация специальной технологии обеспечения целостности БНД, которая позволит полностью или частично реализовать выделенные особенности и свойства. Также не в полной мере решены вопросы обеспечения правильности состава, содержания и организации взаимодействия ИР различной природы. Основной нерешенной частью проблемы обеспечения целостности следует признать отсутствие моделей и методов, позволяющих обеспечить правильность состава и содержания документов как источников входной, промежуточной и выходной информации ИС. В частности, уникальных решений требует организация проверки правильности состава, содержания и организации взаимодействия различных документов, а также документов и БД ИС.

Выделенные проблемы являются следствием недостаточных исследований в области обеспечения целостности документов как ИР ИС и, в частности, целостности базы НД предприятия. В публикациях зарубежных исследователей, например, Л. Кэмпбелла, Ч. Мейджорс, Дж. Дейта целостность данных рассматривается главным образом как точность и корректность информации, которая содержится в БД, с учетом определенных ограничений целостности, а ЦИ анализируется в составе обеспечения ИБ.

Вопросами анализа НД занимаются и российские исследователи. В работах Родичева Ю.А., Лифица И.М., Бобылевой М.П., Куриленко А.Н., Демина Ю.М. рассмотрены различные аспекты формирования, функционирования и прекращения использования внешних и внутренних НД предприятия. Однако в данных и ряде других исследований недостаточно полно раскрыты вопросы формирования и использования БНД предприятия как отдельной составляющей документооборота. Также слабо формализованы и исследованы вопросы свойств и особенностей БНД.

Для оптимальной организации обеспечения безопасности и целостности информации и, в частности, документов предприятия анализируются различные подходы и методы решения этой задачи. В работах Ясенева В.Н., Ярочкина В.И., Вострецовой Е.И. исследуются угрозы ИР и способы защиты информации. Процессы идентификации и аутентификации пользователей, а также методы разграничения доступа рассматривают Скакун В.В., Цирлов В.Л., Голиков А.М. Криптографические методы защиты информации анализируются в работах Ященко В.В., Гатченко Н.А. Управление транзакциями, целостность сущности, ссылочная целостность рассматриваются Голицыной О.Л., Новиковым Б.А., Кузнецовым С.Д., Куликовым С.С. Нужно отметить, что рассмотренные подходы и методы сосредоточены преимущественно на обеспечении точности и правильности данных в БД, а также на подтверждении авторства и защите документов (в том числе нормативных) от НСД. Таким образом, проблема обеспечения правильности состава, содержания и организации взаимодействия ИР различной природы остается не вполне решенной.

В современных публикациях посвященных обеспечению ЦИ (данных) и, в частности, документов как ИР ИС исследуется ряд подходов и методов решения данной проблемы. Так особенности резервного копирования данных с дальнейшим их хранением и восстановлением анализируются в работах Пушкарева А.В., Диченко С.А., Финько О.А., Киселева Д.В. Методы (в том числе криптографические) обеспечения целостности и подлинности информации содержащейся в электронном либо бумажном документе, а также идентификацию и аутентификацию авторов рассматривают Бородин А.В., Еременко А.В., Сагайдак Д.А., Бобылева М.П., Лапина Т.И. Лачихина А.Б. на примере SQL Server рассматривает механизмы обеспечения целостности данных в современных СУБД. Модель мандатного контроля целостности данных на примере микроядерной операционной системы KasperskyOS анализируется Буренковым В.С.

Современные прикладные решения также включают задачи обеспечения безопасности и целостности информации. Методы и механизмы контроля целостности в рамках продукта «1С Предприятие» рассматривают Радченко М.Г., Бойко Э.В., Филатова В.О. В частности, это многоуровневая аутентификация пользователей, защита передаваемой информации от НСД, управление доступом, изоляция транзакций, резервное копирование информационных баз. Свои решения в виде ERP продуктов предлагает компания SAP AG, их анализ представлен в работах Елашкина М., Кале В., Ненашева С.А. Это система проверки полномочий каждого пользователя, с допуском к данным только лиц имеющих на это право, обеспечение безопасности соответствующими профилями и авторизациями, специальные программные интерфейсы криптографической защиты данных. Подходы к решению задачи обеспечения ЦИ (данных) в СЭД «ДЕЛО» исследуют Кугушева Т.В., Ушаков Н.О., Приходько Ю.С. В частности, это специальные модули такие как «КАРМА» и «Мастер паролей», использование ЭЦП и

шифрования, двухфакторная аутентификация, системы защиты корпоративных баз данных и информации на серверах. Также все функции ведения электронного документооборота предприятия обеспечивают ECM системы ELMA и LanDocs, особенности которых анализируют Власова Л.А., Чебескова С.А., Семенова А.А., а также Веселков А.Н., Мотовиц Т.Г., Романов Д.А. Это настройки прав доступа к информации и модулям системы, криптографические методы защиты, прежде всего ЭЦП, ведение полной статистики по каждому документу и системным событиям для обеспечения ИБ, механизмы шифрования конфиденциальных данных для защиты от НСД, протокол действий пользователей в специальном журнале безопасности.

Исходя из сделанных выводов и анализа литературных источников, посвященных теме обеспечения целостности информации (данных) можно считать, что основная цель данной диссертации – разработка новых и усовершенствование существующих моделей и методов обеспечения целостности нормативной документации предприятия, позволяющих унифицировать операции по обеспечению целостности нормативных документов в рамках сервис-ориентированной информационной системы управления предприятием.

Для достижения поставленной цели необходимо выполнить следующие задачи:

– провести обзор и анализ существующих подходов, моделей, методов и способов обеспечения целостности документов предприятия;

– разработать модели целостности нормативной базы предприятия;

– разработать методы обеспечения целостности нормативной базы предприятия;

– разработать информационную технологию обеспечения целостности нормативной базы предприятия и проверить ее работоспособность на практическом примере.

2 МОДЕЛИ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ БАЗЫ НОРМАТИВНЫХ ДОКУМЕНТОВ

2.1 Задача обеспечения целостности базы нормативных документов предприятия

Понятие целостности является фундаментальным в области информационной безопасности и теории баз данных и включает ряд специфических свойств, связанных с таким объектом, как данные. При этом теория баз данных рассматривает ссылочную целостность и целостность данных в аспекте возможности использования данных для их дальнейшей корректной обработки, информационная безопасность - в аспекте сохранения свойств надежности и защищенности данных.

Информация на стадии данных характеризуется определенной формой представления и дополнительной характеристикой, выражаемой термином "структура". В результате, как уже отмечалось, под целостностью информации понимается неискаженность, достоверность, полнота, адекватность, т.е. такое ее свойство, при котором ее содержание и структура определены и изменяются только уполномоченными лицами и процессами.

С учетом специфики используемых механизмов обеспечения целостности данных можно выделить стороны этого понятия в отношении соответствующих видов данных в компьютерных системах. Правильность – заключается в отсутствии логических ошибок в структуре и ошибок в содержании (в значениях) данных при их обработке. Неискаженность – отсутствие подделки данных или возникновения ошибок в данных при их передаче в линиях связи, а также при хранении в компьютерных системах. Неизменность - заключается в тождественности данных определенному эталону.

Для того, чтобы уяснить степень влияния нарушений информационной безопасности на защищаемую информацию и выявить принципы построения систем защиты целостности нормативной базы, необходимо провести системные исследования процессов защиты. В общем случае, любой процесс обработки информации I_k выполняемый в области обработки $O(I_k)$ системы информационного обеспечения деятельности предприятия протекает в условиях воздействия разнообразных дестабилизирующих факторов и угроз $\{F_j\}$ нарушения информационной безопасности, искажающих в большей или меньшей степени предписанный порядок и ход исполнения обработки, представленные на рисунке 2.1. Для противодействия угрозам информации могут быть использованы специальные средства защиты $\{Z_s\}$, обеспечивающие нейтрализацию дестабилизирующих воздействий и угроз.

Наличие дестабилизирующих факторов и угроз $\{F_j\}$ и их воздействие на систему информационного обеспечения и область обработки $O(I_k)$ информации I_k в ней приводит к тому, что существует некоторая потенциальная вероятность $P_{k,i,r}$ негативного воздействия j-го фактора (угрозы) на k-й информационный объект I_k в r-м его состоянии.

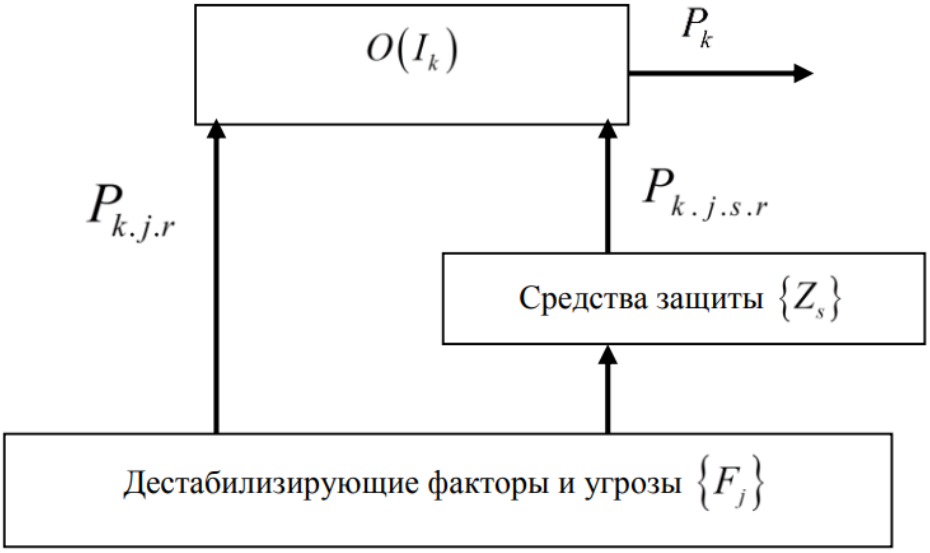

Рисунок 2.1 – Общая модель процесса обеспечения целостности информации

Использование средств защиты между дестабилизирующими источниками и системой информационного обеспечения позволяет уменьшить значение $P_{k,i,s,r}$, т.к. появляется вероятность предупреждения (нейтрализации) воздействия j-й угрозы на k-й информационный объект I_k в r-м его состоянии применением s-го средства защиты.

В большинстве случаев, в первом приближении, можно считать, что характер и уровень воздействия одних негативных факторов не зависит от характера и уровня влияния других, т.е. дестабилизирующие факторы и угрозы являются независимыми друг от друга. Точно так же и средства защиты можно считать, в первом приближении, взаимонезависимыми. Приведенное описание привлекает своей простотой. Достаточно знать вероятностные характеристики дестабилизирующих воздействий $\{F_j\}$ на информационные объекты со стороны различных неблагоприятных факторов и угроз и можно оценить степень защищенности целостности нормативной базы.

Следующей ступенью развития общей модели системы защиты является ее обобщенная модель, Для этого, в соответствии с базовой концепцией кибернетики, вычленим в системе информационного обеспечения предприятия объект управления и средства управления.

Объект управления представляет собой организованную часть системы, вычлененную из нее и соответствующую функциональному предназначению. В рамках исследуемой системы обеспечения целостности информации объектом управления являются как пассивные компоненты информационной системы (носители информации, средства управления носителями, средства взаимодействия с носителями), так и активные системные составляющие – область обработки информации (ресурсы и процессы обработки, необходимые для реализации информационных процедур и операций в соответствии с предназначением и активизируемым режимом функционирования информационной системы).

Управляющей компонентой является система программно-аппаратного управления областью обработки, включающая непосредственно программные компоненты и средства формирования управляющих процессов и процедур.

Для описания объекта управления введем некоторое метрическое пространство $W^{(o)}$, без детализации его структуры. Введение метрики на множестве состояний необходимо для конкретизации понятия близости через меру расстояния на этом множестве. Так как процессы, происходящие в объекте управления, развиваются во времени t, то множество O, образующее пространство $W^{(o)}$, есть множество состояний $S^{(o)}(t)$ объекта: $S^{(o)}(t)$ подмножество O. На данном множестве можно однозначно задать некоторое текущее объективное состояние объекта управления.

Введем также множество управлений $U^{(o)}$, под которыми будем понимать процесс целенаправленных воздействий на управляемый объект со стороны отмеченной системы управления.

Тогда, учитывая, что целевым назначением управляемой подсистемы (пассивных и активных компонент информационной системы) является обработка информационных объектов $\{I_k\}$, ее поведение, при отсутствии воздействия дестабилизирующих факторов $\{F_j\}\equiv F$, можно описать следующим оператором: $a_0: T \times I_k \times R^{(O)} \times U^{(O)} \Longrightarrow I_k^*$, где $\{I_k\}$ – множество состояний информационного объекта I_k, в которые I_k переходит после отрабатывания управлений $U^{(o)}$ с помощью системных ресурсов $R^{(o)}$, в компонентах тракта обработки информации (носители информации – средства управления носителями – средства взаимодействия с носителями – область обработки).

Причем, оператор обеспечения долговременного хранения объектов $\{I_k\}$ (оператор носителя информации или информационного хранилища) есть: $\chi: T \times \{I_k\} \times G_k \Longrightarrow I_k$. Здесь $\{G_k\}$ – множество управляющих воздействий, необходимых для выбора соответствующего информационного объекта I_k из хранилища перед его отправкой на обработку. Множество системных ресурсов $R^{(o)} \equiv\{ R^{(\delta)}, R^{(\zeta)}, R^{(\alpha)}\}$, – есть множество аппаратных и системных программных средств, необходимых для осуществления обработки объекта I_k, при этом: $R^{(\delta)}$ – ресурсы, обеспечивающие функционирование средств управления носителем информации; $R^{(\zeta)}$ – ресурсы, необходимые для организации взаимодействия с носителем информации; $R^{(\alpha)}$ – ресурсы, обслуживающие область обработки информации.

Построение множества программ $P^{(o)}$ обработки информационных объектов $\{I_k\}$ осуществляется на основе сведений о характере обрабатываемых информационных объектах I_k (точнее об объектах $I_k^{(\zeta)}$, поступающих в область обработки), цели ее обработки I_k^C и предварительно загруженного из хранилища информационного массива $I_k^{(P)}$, представляющего собой программный код информационной технологии обработки.

Можно смело утверждать при этом, что, если процессы управления областью обработки информации $U^{(o)}$ и ресурсами $U^{(\varepsilon)}$, (а через ресурсы и трактом доставки объектов I_k к области обработки), реализуется корректно, без сбоев и искажений, то справедливо утверждение $I_k^* \rightarrow I_k^C$.

Рассмотренные отношения дают отображение процессов, протекающих в системе информационного обеспечения предприятия в предположении, что влияние негативных воздействий F отсутствует или очень мало. В реальных же условиях эксплуатации нормативной базы как информационной системы влиянием факторов F пренебрегать нельзя, причем их воздействию обычно подвергаются как управляемые объекты (средства управления носителем, средства взаимодействия с носителем, область обработки информации) так и управляющая подсистема (компоненты воспроизведения программного обеспечения, формирователь управляющих воздействий, ресурсы), а также информационные объекты I_k, находящиеся в информационном хранилище.

Из полученной модели видно, что для построения эффективной системы обеспечения целостности основного тракта обработки информации нормативной базы необходимо обеспечить как защиту самого тракта, так и защиту ресурсов, программ и управлений. Для этого следует сформировать корректирующие воздействия на защищаемые объекты и области информационной системы. Для обеспечения аудита за состоянием информационной системы обеспечения целостности нормативной базы, за работой средств обеспечения целостности система должна быть оснащена необходимыми компонентами контроля, данные от которых учитываются при определении текущей стратегии обеспечения целостности нормативной базы [35, с. 348].

Приведенное в [21, с. 6] определение понятия «целостность ресурсов ИС» разделяет задачу обеспечения целостности ИР на две отдельные подзадачи:

а) подзадача обеспечения изменения ИР субъектами ИС, имеющими на это право (подзадача №1);

б) подзадача обеспечения сохранения состава, содержания и организации взаимодействия ресурсов ИС между собой и с другими ресурсами ИС (подзадача №2).

Следует отметить, что в теории БД эти две подзадачи представляют собой следующие самостоятельные задачи [53, с. 58]:

а) задача защиты данных как предотвращения доступа к ним со стороны несанкционированных пользователей;

б) задача поддержки целостности данных как предотвращения их разрушения при доступе со стороны санкционированных пользователей.

Эти задачи в целом решены для каждой конкретной СУБД. Поэтому будем исходить из предположения, что БД ИС является основным инструментом, используемым для хранения НД предприятия. Данное предположение позволяет в дальнейшем использовать для реализации моделей и методов обеспечения целостности БНД предприятия протестированные и многократно апробированные инструментальные средства СУБД.

Использование этого предположения позволяет представить модель целостности БНД как ИР в виде набора предикатов по аналогии с моделью обеспечения целостности БД [53, с. 61].

Рассмотрим вначале задачу обеспечения целостности отдельного НД как самостоятельного ИР предприятия. Целостность отдельного НД d_i следует рассматривать как состояние документа d_i, в котором состав, содержание и взаимодействие с другими НД предприятия являются:

а) неизменными;

б) достоверными;

в) определенными субъектами ИС, имеющими на это право.

Неизменность НД d_i определяется как невозможность внесения изменений в описания состава, содержания и взаимодействия данного документа с другими НД за период актуальности данного НД. Под периодом актуальности НД d_i здесь и в дальнейшем будем понимать промежуток времени $[\tau_b, \tau_e]$, устанавливающий даты и время начала и окончания использования НД d_i в СУП. Достоверность НД d_i определяется как существование конкретных элементов описаний состава, содержания и взаимодействия данного документа с другими НД за период актуальности данного НД, причем эти элементы должны быть определены субъектами ИС, имеющими на это право. Определенность НД d_i субъектами ИС, имеющими на это право определяется как множество описаний субъектов ИС, которым руководством предприятия через администраторов ИС делегировано право формировать и изменять состав, содержание и взаимодействие с другими НД конкретного НД d_i.

Под субъектами ИС, которые имеют право формировать и изменять НД d_i здесь и в дальнейшем будем понимать:

а) пользователей (операторов) ИС, обеспечивающих ввод в ИС новых данных о составе НД d_i, о содержании НД d_i, а также о взаимодействии НД d_i с другими НД, входящими в БНД предприятия;

б) IT-сервисы, реализующие отдельные функции ИС по формированию, обработке и отображению НД d_i, а также по пересылке НД d_i другим IT-сервисам ИС.

Такое представление позволяет определить целостность как систему предикатов, описывающих:

а) неизменность состава НД d_i за период актуальности данного НД;

б) неизменность содержания НД d_i за период актуальности данного НД;

в) неизменность взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД;

г) определенность пользователей ИС, имеющих право изменять НД d_i за период актуальности данного НД;

д) определенность IT-сервисов ИС, имеющих право изменять НД d_i за период актуальности данного НД;

е) достоверность состава НД d_i за период актуальности данного НД;

ж) достоверность содержания НД d_i за период актуальности данного НД;

и) достоверность взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД.

Истинность предикатов, описывающих достоверность состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД, подтверждает, что в БНД не существует записей о НД d_i, в которых бы состав, содержание или взаимодействие данного НД с другими НД из БНД различались бы за указанный период актуальности. Истинность предикатов, описывающих неизменность состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД, подтверждает, что в БНД не вносились кем-либо такие сведения о НД d_i, которые бы изменяли описания состава, содержания или взаимодействий данного НД с другими НД из БНД за указанный период актуальности. Выделение достоверности и неизменности как отдельных характеристик целостности БНД в данном случае оправдано тем, что не существует единого источника НД, используемых на предприятии. Поэтому существует отличная от нуля вероятность возникновения ситуации, когда сформированные различными источниками НД d_i и НД d_j будут неизменными, но не достоверными (например, в результате того, что один и тот же элемент НД d_i и НД d_j будет иметь в этих документах разные значения).

Формально данную систему предикатов следует представить таким образом:

$$P_{Integrity_{d_i}} = \begin{cases} P_{cons_{d_i}}; \\ P_{cont_{d_i}}; \\ P_{inter_{d_i}}; \\ P_{user_{d_i}}; \\ P_{serv_{d_i}}; \\ P_{acc\_cons_{d_i}}; \\ P_{acc\_cont_{d_i}}; \\ P_{acc\_inter_{d_i}}, \end{cases} \quad (2.1)$$

где $P_{cons_{d_i}}$ – предикат, определяющий неизменность состава НД d_i за период актуальности данного НД;

$P_{cont_{d_i}}$ – предикат, определяющий неизменность содержания НД d_i за период актуальности данного НД;

$P_{inter_{d_i}}$ – предикат, определяющий неизменность взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД;

$P_{user_{d_i}}$ – предикат, определяющий пользователей ИС, имеющих право изменять НД d_i за период актуальности данного НД;

$P_{serv_{d_i}}$ – предикат, определяющий IT-сервисы ИС, имеющие право изменять НД d_i за период актуальности данного НД;

$P_{acc\_cons_{d_i}}$ – предикат, определяющий достоверность состава НД d_i за период актуальности данного НД;

$P_{acc\_cont_{d_i}}$ – предикат, определяющий достоверность содержания НД d_i за период актуальности данного НД;

$P_{acc\_inter_{d_i}}$ – предикат, определяющий достоверность взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД.

Тогда задачу обеспечения целостности БНД предприятия можно в общем случае представить следующим образом:

$$\forall d_i \in NDB \exists P_{Integrity_{d_i}} = \begin{cases} P_{cons_{d_i}} = 1; \\ P_{cont_{d_i}} = 1; \\ P_{inter_{d_i}} = 1; \\ P_{user_{d_i}} = 1; \\ P_{serv_{d_i}} = 1; \\ P_{acc\_cons_{d_i}} = 1; \\ P_{acc\_cont_{d_i}} = 1; \\ P_{acc\_inter_{d_i}} = 1. \end{cases} \quad (2.2)$$

где NDB – множество НД, образующих БНД предприятия.

Данную задачу следует понимать как задачу обеспечения для любого НД d_i, включаемого в БНД предприятия, истинности каждого из предикатов выражения (2.1), характеризующих отдельные аспекты целостности данного НД.

Однако предложенная модель задачи обеспечения целостности БНД предприятия (2.2) носит общий характер. Для ее детализированного описания необходимо разработать формальные описания НД и субъектов ИС, имеющих право изменять НД.

2.2 Разработка моделей и метода обеспечения неизменности базы нормативных документов

Для детализированных описаний предикатов $P_{cons_{d_i}}$, $P_{cont_{d_i}}$ и $P_{inter_{d_i}}$, определяющих неизменность состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия, необходимо разработать декларативную модель НД d_i, которая могла бы формально описать указанные характеристики НД как ИР СУП. В основу подобной модели предлагается поместить фреймовую модель. Применение данной модели обусловлено следующими соображениями [92]:

– использование фреймовой модели знаний позволяет применять единый математический аппарат как для описания знаний о ПрО в виде НД, так и для

описания знаний, реализованных в элементах ИС в виде моделей программного обеспечения данной ИС;

– использование фреймовой модели позволяет реализовать взаимно-однозначное отображение представлений НД в представления элементов программного обеспечения ИС (в методологии объектно-ориентированного программирования понятие фрейма соответствует классу [93]).

Кроме того, поскольку значительное количество современных СУБД основано на реляционной модели данных, применение фреймовой модели знаний позволяет осуществить в результате решения задачи объектно-реляционного отображения последующее взаимно-однозначное отображение представлений НД и элементов программного обеспечения ИС в элементы информационного обеспечения этой ИС [94, 95].

Для формального описания фрейма fr используем приведенную в [96] теоретико-множественную модель, которая имеет следующий вид:

$$fr = \{ n, [(ns_1, vs_1, ps_1), (ns_2, vs_2, ps_2), \ldots, (ns_k, vs_k, ps_k)] \}, \qquad (2.3)$$

где n – имя фрейма;

(ns, vs, ps) – слот фрейма;

k – количество слотов фрейма;

ns_i – имя слота, $i = \overline{1,k}$;

vs_i – значение слота, $i = \overline{1,k}$;

ps_i – имя присоединенной процедуры, $i = \overline{1,k}$.

В качестве элемента слота «имя присоединенной процедуры» в фреймах используется подпрограмма процедурного типа. Присоединённым процедурам в ООП соответствуют методы классов, в реляционных базах данных им соответствуют связанные с таблицами триггеры, процедуры и функции [97].

Однако такое формальное описание позволяет определить только отдельный экземпляр НД d_i. Причиной этого является необходимость в процессе описания НД d_i как фрейма моделью (2.3) явно указывать конкретные значения каждого слота этого фрейма. Кроме того, для описания состава документа нет необходимости указывать все присоединенные процедуры фрейма, описывающего НД d_i. Поэтому предлагается в описании НД d_i заменить описания конкретных значений слотов фрейма и присоединенных процедур описанием типа соответствующего слота как домена (множества допустимых значений), из которого данный слот может принимать определенные значения. Такое описание позволяет использовать в дальнейшем для прикладного решения задачи обеспечения целостности БНД различные варианты реализации ограничений целостности уровня домена [53, с. 518].

Для описания взаимодействия НД d_i с другими НД введем понятие связи фреймовых моделей, описывающих эти НД. Данное понятие позволяет описывать различные виды взаимодействия НД однотипным формальным описанием.

Кроме того, предлагается выделить в отдельное формальное описание такой вид взаимодействия НД, как тождественность. Данный вид взаимодействия возможен в случае, когда вносимые в состав и содержание НД изменения приводит к появлению новых вариантов описания данного НД, не прекращая период актуальности данного НД. Кроме того, данный вид взаимодействия позволяет решить проблему синонимии различных описаний НД.

С учетом предложенных дополнений, основанная на фреймовой модели знаний модель НД как элемента БНД предприятия будет представлена как кортеж следующего вида [98, 99]:

$$d_i = \left\langle n_i, \left\{ \left\langle n_i^x, T_i^x \right\rangle \right\}, \left(R_{d_k}^{d_i} \right), \left(\varphi_{d_k}^{d_i} \right) \right\rangle, \tag{2.4}$$

где n_i – атрибут, описывающий уникальное обозначение НД d_i;

n_i^x – атрибут, описывающий уникальное обозначение x-го элемента a_i^x НД d_i, $x = \overline{1,N}$, где N – количество элементов в описании НД d_i;

T_i^x – атрибут, описывающий тип x-го элемента a_i^x НД d_i (тип элемента может быть одним из множества простых типов данных или сложным (определяемым автором документа));

$R_{d_k}^{d_i}$ – множество кортежей атрибутов, устанавливающих факт существования связей различных типов (ассоциация, агрегация, композиция, обобщение, зависимость) между НД d_i и НД d_k, каждый элемент которого имеет вид [98, p. 17; 99, с. 63]:

$$R_{d_k}^{d_i} = \left\langle n_r, \left\{ \left\langle n_i^y, T_i^y \right\rangle \right\}, \left\{ \left\langle n_k^y, T_k^y \right\rangle \right\}, Pow_{d_i}^R, Pow_{d_k}^R, S_{d_i}^R, S_{d_k}^R \right\rangle, \tag{2.5}$$

где n_r – уникальное наименование связи, существующей между НД d_i и НД d_k;

$\{\langle n_i^y, T_i^y \rangle\}$ – подмножество атрибутов НД d_i, которое участвует в образовании связи $R_{d_k}^{d_i}$, $\{\langle n_i^y, T_i^y \rangle\} \subseteq \{\langle n_i^x, T_i^x \rangle\}$;

$\{\langle n_k^y, T_k^y \rangle\}$ – подмножество атрибутов НД d_k, которое участвует в образовании связи $R_{d_k}^{d_i}$, $\{\langle n_k^y, T_k^y \rangle\} \subseteq \{\langle n_k^x, T_k^x \rangle\}$;

$Pow_{d_i}^R$ – атрибут, описывающий мощность связи $R_{d_k}^{d_i}$ для НД d_i, который принимает целочисленные положительные значения, соответствующие количеству описаний НД d_i, участвующих в образовании связи $R_{d_k}^{d_i}$;

$Pow_{d_k}^R$ – атрибут, описывающий мощность связи $R_{d_k}^{d_i}$ для НД d_k, который принимает целочисленные положительные значения, соответствующие количеству описаний НД d_k, участвующих в образовании связи $R_{d_k}^{d_i}$;

$S_{d_i}^R$ – атрибут, описывающий степень участия экземпляров НД d_i в

образовании связи $R_{d_k}^{d_i}$, который принимает значение 0, если связь со стороны НД d_i носит необязательный характер, или 1, если связь со стороны НД d_i носит обязательный характер;

$S_{d_k}^{R}$ – атрибут, описывающий степень участия экземпляров НД d_k в образовании связи $R_{d_k}^{d_i}$, который принимает значение 0, если связь со стороны НД d_k носит необязательный характер, или 1, если связь со стороны НД d_k носит обязательный характер;

$\varphi_{d_k}^{d_i}$ – множество кортежей атрибутов, устанавливающих факт тождественности НД d_i и НД d_k, каждый элемент которого имеет вид [92, с. 129-132; 98, p. 15-22; 99, с. 55-71]:

$$\varphi_{d_k}^{d_i} = \left\langle Id_{\varphi}, n_i, n_k, (R_{ik}) \right\rangle, \tag{2.6}$$

где Id_{φ} – идентификатор связи, описанной в общем случае выражением (2.5) и устанавливающей тождественность НД d_i и НД d_k;

n_k – атрибут, описывающий уникальное обозначение НД d_k, являющегося тождественным НД d_i;

(R_{ik}) – множество связей, описанных кортежами (2.5), в которых участвуют НД d_i и НД d_k.

Связь, устанавливающая тождественность НД d_i и НД d_k, в общем случае определяется как обязательная связь «один к одному» между НД d_i и НД d_k и описывается следующим образом:

$$\varphi_{d_k}^{d_i} = \left\langle Id_{\varphi}, \left\{ \left\langle n_i^y, T_i^y \right\rangle \right\}, \left\{ \left\langle n_k^y, T_k^y \right\rangle \right\}, 1,1,1,1 \right\rangle. \tag{2.7}$$

Предложенная модель (2.4)-(2.6) позволяет формально описать состав НД d_i, множество его возможных содержаний, а также возможные взаимодействия с другими НД, определяемые либо через установление фактов связей между НД d_i и НД d_k, либо через установление фактов тождественности описаний НД d_i и НД d_k. Множество возможных содержаний НД d_i определяется в модели (2.4)-(2.6) через задание типов каждого конкретного атрибута a_i^x НД d_i.

На основании модели (2.4)-(2.6) становится возможным представить модель БНД предприятия как результат объединения в рамках этой базы моделей всех НД d_i, *i=1,…,N*. Такая модель формально будет описываться следующим выражением [98, p. 18]:

$$BND = \bigcup_i \left\langle n_i, \left\{ \left\langle n_i^x, T_i^x \right\rangle \right\}, \left(R_{d_k}^{d_i} \right), \left(\varphi_{d_k}^{d_i} \right) \right\rangle; i,k = 1,\dots,N; i \neq k. \tag{2.8}$$

Использование модели (2.4)-(2.6) позволяет детализированно описать предикат $P_{cons_{d_i}}$ следующим образом:

$$P_{cons_{d_i}} = (n_i^1, \dots, n_i^x, \dots, n_i^N, \tau_{bi}, \tau_{ei}), \quad (2.9)$$

где τ_{bi} – дата и время начала использования НД d_i в СУП;

τ_{ei} – дата и время окончания использования НД d_i в СУП.

Предикат (2.9) определяет состав НД d_i как набор атрибутов, образующих структуру НД d_i на протяжении периода актуальности НД d_i $[\tau_{bi}, \tau_{ei}]$. Предикат (2.8) будет истинным при условии, что этот набор остается неизменным на протяжении периода актуальности НД d_i $[\tau_{bi}, \tau_{ei}]$.

Предикат $P_{cont_{d_i}}$ с использованием модели (2.4)-(2.6) будет детализированно описан следующим образом:

$$P_{cont_{d_i}} = \left(\langle n_i^1, T_i^1\rangle, \dots, \langle n_i^x, T_i^x\rangle, \dots \langle n_i^N, T_i^N\rangle, \tau_{bi}, \tau_{ei}\right). \quad (2.10)$$

Предикат (2.10) определяет множество содержаний НД d_i как домены (множества допустимых значений) для каждого типа каждого атрибута n_i^x, $x = 1, \dots, N$, входящего в состав НД d_i. являются Предикат (2.10) будет истинным при условии, что каждый атрибут n_i^x НД d_i на протяжении периода актуальности НД d_i $[\tau_{bi}, \tau_{ei}]$ принимает допустимое значение из домена соответствующего этому атрибуту типа T_i^x.

С учетом взаимодействий НД d_i с другими НД БНД предприятия, конкретные виды которых определяются вариантами описаний связей (2.5) и кортежей тождественности (2.6), предлагается рассматривать предикат $P_{inter_{d_i}}$ как систему следующих предикатов:

$$P_{inter_{d_i}} = \begin{cases} P_{R_{d_i}}; \\ P_{\varphi_{d_i}}, \end{cases} \quad (2.11)$$

где $P_{R_{d_i}}$ – предикат, определяющий существование связей между НД d_i и другими НД БНД предприятия;

$P_{\varphi_{d_i}}$ – предикат, определяющий тождественность описаний НД d_i и других НД БНД предприятия.

Предикат $P_{R_{d_i}}$ с использованием модели (2.4)-(2.6) будет детализированно описан следующим образом:

$$P_{R_{d_i}} = \left(P_{R_{d_1}^{d_i}}, \dots, P_{R_{d_k}^{d_i}}, \dots, P_{R_{d_N}^{d_i}}, \tau_{bi}, \tau_{ei}\right)_{i \neq k}, \quad (2.12)$$

где $P_{R_{d_k}^{d_i}}$ – предикат, описывающий существование связи между НД d_i и НД d_k, представленной выражением (2.5), имеющий следующий вид:

$$P_{R_{d_k}^{d_i}} = \left(n_r, \left\{ \left\langle n_i^y, T_i^y \right\rangle \right\}, \left\{ \left\langle n_k^y, T_k^y \right\rangle \right\}, Pow_{d_i}^R, Pow_{d_k}^R, S_{d_i}^R, S_{d_k}^R \right)_{i \neq k}. \quad (2.13)$$

Предикат (2.13) определяет взаимодействия НД d_i как связи между НД d_i и другими НД, образующими БНД предприятия. Предикат (2.13) будет истинным при условии, что каждый из предикатов $P_{R_{d_k}^{d_i}}$ будет истинным на протяжении периода актуальности НД d_i $[\tau_{bi}, \tau_{ei}]$.

Предикат $P_{\varphi_{d_i}}$ с использованием модели (2.4)-(2.6) будет детализированно описан следующим образом:

$$P_{\varphi_{d_i}} = \left(P_{\varphi_{d_1}^{d_i}}, \dots, P_{\varphi_{d_k}^{d_i}}, \dots, P_{\varphi_{d_N}^{d_i}}, \tau_{bi}, \tau_{ei} \right)_{i \neq k}, \quad (2.14)$$

где $P_{\varphi_{d_k}^{d_i}}$ – предикат, описывающий факт тождественности описаний НД d_i и НД d_k, представленной выражением (2.6), имеющий следующий вид:

$$P_{R_{d_k}^{d_i}} = \left(Id_\varphi, n_i, n_k, \left(R_{ik} \right) \right)_{i \neq k}. \quad (2.15)$$

Предикат (2.15) определяет синонимичные варианты описания НД d_i как факты существования тождественности описаний НД d_i и НД d_k, образующими БНД предприятия. Предикат (2.15) будет истинным при условии, что каждый из предикатов $P_{R_{d_k}^{d_i}}$ будет истинным на протяжении периода актуальности НД d_i $[\tau_{bi}, \tau_{ei}]$.

Выражения (2.9), (2.10). (2.12) и (2.14) позволяют разработать метод решения подзадачи обеспечения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия. Данный метод представляет собой последовательность таких этапов.

Этап 1. Выбрать НД d_i и выполнить логическую операцию

$$\langle n_i, \{\langle n_i^x, T_i^x \rangle\}, \left(R_{d_k}^{d_i} \right), \left(\varphi_{d_k}^{d_i} \right) \rangle \wedge \cup_i \left\langle n_i, \left\{ \left\langle n_i^x, T_i^x \right\rangle \right\}, \left(R_{d_k}^{d_i} \right), \left(\varphi_{d_k}^{d_i} \right) \right\rangle. \quad (2.16)$$

Если операция (2.16) принимает значение «истина», то перейти к Этапу 2. В противном случае сообщить об отсутствии описания НД d_i в БНД предприятия и завершить применение метода.

Этап 2. Если для выбранного на Этапе 1 НД d_i $P_{cons_{d_i}} = \left(n_i^1, \dots, n_i^x, \dots, n_i^N, \tau_{bi}, \tau_{ei}\right) = 1$, то перейти к Этапу 3. В противном случае сообщить о нарушении неизменности описания состава НД d_i в БНД предприятия и завершить применение метода.

Этап 3. Если для выбранного на Этапе 1 НД d_i $P_{cont_{d_i}} = \left(\langle n_i^1, T_i^1\rangle, \dots, \langle n_i^x, T_i^x\rangle, \dots \langle n_i^N, T_i^N\rangle, \tau_{bi}, \tau_{ei}\right) = 1$, то перейти к Этапу 4. В противном случае сообщить о нарушении неизменности описания возможного содержания НД d_i в БНД предприятия и завершить применение метода.

Этап 4. Если для выбранного на Этапе 1 НД d_i $P_{R_{d_i}} = \left(P_{R_{d_1}^{d_i}}, \dots, P_{R_{d_k}^{d_i}}, \dots, P_{R_{d_N}^{d_i}}, \tau_{bi}, \tau_{ei}\right)_{i \neq k} = 1$, то перейти к Этапу 5. В противном случае сообщить о нарушении неизменности описаний взаимодействия НД d_i с конкретными НД d_k в БНД предприятия и завершить применение метода.

Этап 5. Для выбранного на Этапе 1 НД d_i выполнить логическую операцию:

$$P_{R_{d_i}} = \left(P_{R_{d_1}^{d_i}}, \dots, P_{R_{d_k}^{d_i}}, \dots, P_{R_{d_N}^{d_i}}, \tau_{bi}, \tau_{ei}\right)_{i \neq k} = 1 \vee \varphi_{d_k}^{d_i} = \emptyset. \qquad (2.17)$$

Если операция (2.17) принимает значение «истина», то сообщить об успешном обеспечении неизменности НД d_i и завершить применение метода. В противном случае сообщить о нарушении неизменности тождественности описаний НД d_i и описаний конкретных НД d_k в БНД предприятия и завершить применение метода.

Разработанные модели обеспечения неизменности БНД предприятия в виде детализированных описаний предикатов $P_{cons_{d_i}}$, $P_{cont_{d_i}}$ и $P_{inter_{d_i}}$ выражениями (2.9), (2.10), (2.12) и (2.14) и метод обеспечения неизменности БНД предприятия позволяют автоматизировать процесс проверки неизменности состава, содержания и взаимодействия любого НД d_i, описанного моделью (2.4)-(2.6), в рамках действующей на предприятии БНД, представленной в виде выражения (2.8).

2.3 Разработка моделей и метода определения субъектов информационной системы, имеющих права изменять базу нормативных документов

Как было показано в подразделе 2.1, основными субъектами ИС, имеющими право изменять НД, входящие в БНД предприятия, являются пользователи ИС и IT-сервисы, с помощью которых пользователи ИС выполняют над НД операции по формированию, обработке, отображению и пересылке. При этом следует отметить, что перечень пользователей ИС, как и перечень IT-сервисов ИС, имеющих право изменять НД, может меняться за период актуальности данного НД. Однако существует период актуальности

описаний этих пользователей и IT-сервисов, поскольку за время функционирования предприятия пользователи, как и отдельные IT-сервисы могут меняться.

Следует также учесть, что пор отношению к жизненному циклу НД любой пользователь ИС, взаимодействующий с БНД, может быть отнесен к одному из следующих классов:

а) автор НД, выполняющий операции создания, модификации и удаления описаний состава, содержания и взаимодействий НД с другими НД из БНД предприятия, а также определяющий дату и время создания НД и отдельных его экземпляров;

б) лицо, утверждающее НД, определяющее дату и время начала действия НД и отдельных его экземпляров;

в) читатель НД, использующий содержание НД в ходе выполнения своих процессов.

При этом только авторы НД имеют все права на изменение состава, содержания и взаимодействия данного НД с другими НД, входящими в БНД предприятия. Лица, утверждающие НД, могут давать рекомендации по возможному изменению отдельных НД, но в силу занимаемых должностей (обычно это представители высшего руководства предприятия) не имеющие возможности лично выполнять работу по такому изменению. Читатели НД могут только читать сформированные экземпляры НД, но не могут (прежде всего, на уровне хранимых данных по каждому атрибуту конкретного НД) непосредственно изменять состав, содержание и взаимодействие данного НД с другими НД, входящими в БНД предприятия.

Поэтому для решения подзадачи №1 предлагается ввести модель авторов НД, позволяющую формально описать одного или нескольких сотрудников предприятия как лиц, имеющих права на создание, чтение, модификацию и удаление описаний НД из БНД. Данная совокупность прав перекрывает все множество операций над описаниями НД в БНД, доступных для выполнения и реализуемых средствами современных информационных технологий.

В общем случае такая модель будет представлена кортежем, имеющим следующий вид:

$$u_{ij} = \langle n_i, S\_name_{ij}, Name_{ij}, Patron_{ij}, Post_{ij}, d\_signature_{ij}, \tau_{bij}, \tau_{eij} \rangle, \quad (2.18)$$

где u_{ij} – обозначение j-го пользователя ИС, имеющего право изменять НД d_i;

n_i – атрибут, описывающий уникальное обозначение НД d_i в описании его состава и содержания (2.4);

S_name_{ij} – атрибут, описывающий фамилию j-го пользователя ИС, имеющего право изменять НД d_i;

$Name_{ij}$ – атрибут, описывающий имя j-го пользователя ИС, имеющего право изменять НД d_i;

$Patron_{ij}$ – атрибут, описывающий отчество j-го пользователя ИС, имеющего право изменять НД d_i;

$Post_{ij}$ – атрибут, описывающий должность j-го пользователя ИС, имеющего право изменять НД d_i;

$d\_signature_{ij}$ – агрегат, представляющий собой кортеж атрибутов, описывающих набор прав j-го пользователя ИС на изменение НД d_i (далее - сигнатура);

τ_{bij} – атрибут, описывающий дату и время включения j-го пользователя ИС в перечень пользователей ИС, имеющих право изменять НД d_i;

τ_{eij} – атрибут, описывающий дату и время исключения j-го пользователя ИС из перечня пользователей ИС, имеющих право изменять НД d_i.

Сигнатура $d\_signature_{ij}$ будет принимать различный вид, который будет зависеть от способа задания прав j-го пользователя ИС на изменение НД d_i. Здесь следует отметить, что конкретная реализация указанных способов может привести к кардинальному изменению способов решения подзадачи № 1. Так, использование для обозначения прав j-го пользователя ИС на изменение НД d_i таких инструментов, как усиленная неквалифицированная и усиленная квалифицированная ЭЦП, делают разработку специализированных моделей и методов решения задачи обеспечения целостности нецелесообразными, поскольку сводят решение данной задачи к проверке криптографического преобразования информации с использованием специального ключа. Такие ЭЦП позволяют [100]:

а) определить лицо, подписавшее электронный документ;

б) обнаружить факт внесения изменений в электронный документ после момента его подписания.

Поэтому в данной диссертационной работе основное внимание уделяется решению задачи обеспечения целостности БНД предприятия, которые создаются и изменяются сотрудниками, имеющими неквалифицированную ЭЦП или же использующими другие механизмы ИС, удостоверяющие их личность (например, механизмы присвоения и обновления паролей доступа к данным и т.п.).

Для описания в качестве субъектов ИС, имеющих права на изменение НД, IT-сервисов данной ИС следует учесть такие соображения:

а) под IT-сервисом следует понимать совокупность различных средств комплекса средств автоматизации, реализующих законченную операцию предоставления или обработки данных, переводя их из одного целостного состояния в другое, используя при этом стандартные платформо-независимые интерфейсы [92, с. 131; 101];

б) для любого пользователя и администратора ИС IT-сервисы представляются элементами ИС, состояния и операции которых закрыты для вмешательства извне [101, с. 367];

в) судить о документах и структурах данных, которые обрабатываются IT-сервисом, пользователи и администраторы ИС могут только по описанию входных и выходных сообщений («message»), которые приводятся в WSDL-документах, публикующих IT-сервис в реестре сервисов ИС.

При этом следует помнить, что в самих WSDL-документах используются различные форматы описания сообщений, представлнные на рисунке 2.2 [102].

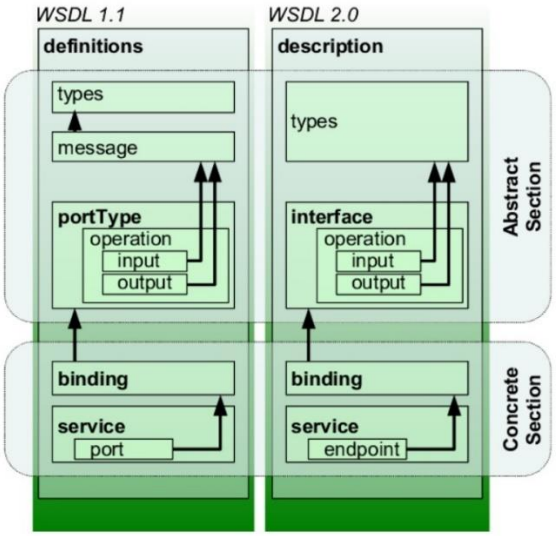

Рисунок 2.2 – Схемы структуры WSDL-документов версий 1.1 и 2.0

В документах, написанных с использованием WSDL v 1.1, для описания структур данных входных и выходных сообщений используется элемент «message». Данный элемент представляет собой набор атрибутов и типов данных этих атрибутов. Типы данных атрибутов могут быть простыми и сложными, для определения которых могут использоваться другие структуры данных [103]. В документах, написанных с использованием WSDL v 2.0, сообщения являются частью описания типов в абстрактной части WSDL-документа [104]. Однако в любом случае входные и выходные сообщения IT-сервиса могут быть описаны как совокупность структур данных, которыми этот IT-сервис обменивается с другими IT-сервисами. Исходя из этого, сервис можно рассматривать как множество вида [105]:

$$s_i = (D_i^r ; D_i^t), \tag{2.19}$$

где s_i – обозначение сервиса;

D_i^r – множество структур данных, которые сервис s_i получает от других сервисов;

D_i^t – множество структур данных, которые сервис s_i передает другим сервисам.

Множество D_i^r можно представить следующим образом [105, с. 63]:

$$D_i^r = (d_{i1}^r, d_{i2}^r, ..., d_{ij}^r, ..., d_{ik}^r),\ j \neq i, \tag{2.20}$$

где k – количество сервисов, образующих множество сервисов, эксплуатируемых в рамках сервис-ориентированной ИС;

d_{ij}^{r} – множество метаданных, описывающих атрибуты данных, значения которых сервис s_i получает от другого сервиса s_j, которое имеет вид [105, с. 64]:

$$d_{ij}^{r} = [at_{ij1}^{r}, at_{ij2}^{r}, ..., at_{ijk}^{r}, ..., at_{ijm}^{r}]; \quad (2.21)$$

где at_{ijk}^{r} – набор метаданных, описывающих атрибут данных, значение которого сервис s_i получает от другого сервиса s_j.

Множество D_i^t аналогично можно представить следующим образом [105, с. 64]:

$$D_i^t = (d_{i1}^t, d_{i2}^t, ..., d_{ij}^t, ..., d_{ik}^t),\ j \neq i, \quad (2.22)$$

где d_{ij}^t – множество метаданных, описывающих атрибуты данных, значения которых сервис s_i передает другому сервису s_j, которое имеет вид [105, с. 65]

$$d_{ij}^t = [at_{ij1}^t, at_{ij2}^t, ..., at_{ijp}^t, ..., at_{ijn}^t]; \quad (2.23)$$

где at_{ijp}^t – набор метаданных, описывающих атрибут данных, значение которого сервис s_i передает другому сервису s_j.

Тогда каждый сервис может быть описан следующим образом [105, с.65]:

$$s_i = \left(\left(\bigcup_{j,k} at_{ijk}^{r} \right); \left(\bigcup_{j,p} at_{ijp}^{t} \right) \right). \quad (2.24)$$

Данную модель предлагается скорректировать для унификации описания атрибутов и типов данных по аналогии с выражением (2.4). Тогда любой атрибут сервиса s_i может быть представлен кортежем

$$at_{ijl} = \langle n_{ijl}, T_{ijl} \rangle, \quad (2.25)$$

где n_{ijl} – обозначение l-го атрибута данных, участвующего в обмене сообщениями между сервисами s_i и s_j;

T_{ijl} – обозначение типа данных l-го атрибута данных, участвующего в обмене сообщениями между сервисами s_i и s_j.

Тогда модифицированная модель IT-сервиса, имеющего право изменять НД, будет иметь следующий вид [98, p. 20]:

$$s_i = \left\langle service\_key_i, \left(\bigcup_{j,k} \left\langle n_{ijk}^r, T_{ijk}^r \right\rangle \right), \left(\bigcup_{j,p} \left\langle n_{ijp}^t, T_{ijp}^t \right\rangle \right), \tau_{bs_i}, \tau_{es_i} \right\rangle, \quad (2.26)$$

где $service\_key_i$ – уникальное обозначение i-го IT-сервиса ИС;

n_{ijk}^r – обозначение k-го атрибута данных, используемого для описания сообщения, передаваемого сервису s_i сервисом s_j;

T_{ijk}^r – обозначение типа данных k-го атрибута данных, используемого для описания сообщения, передаваемого сервису s_i сервисом s_j;

n_{ijp}^t – обозначение p-го атрибута данных, используемого для описания сообщения, передаваемого сервисом s_i сервису s_j;

T_{ijp}^t – обозначение типа данных p-го атрибута данных, используемого для описания сообщения, передаваемого сервисом s_i сервису s_j;

τ_{bs_i} – дата и время начала периода актуальности для IT-сервиса s_i;

τ_{es_i} – дата и время окончания периода актуальности для IT-сервиса s_i;

Предложенные модели позволяют детализированно описать предикат $P_{user_{d_i}}$, определяющий пользователей ИС, имеющих право изменять НД d_i за период актуальности данного НД, следующим выражением:

$$P_{user_{d_i}} = (n_i, d\_signature_{ij}). \quad (2.27)$$

Предикат (2.27) определяет множество сигнатур пользователей ИС, имеющих права на изменение НД d_i. Предикат (2.24) будет истинным при условии, что сигнатура пользователя, изменяющего НД d_i на протяжении периода актуальности данного НД d_i $[\tau_{bi}, \tau_{ei}]$, находится в списке разрешенных сигнатур $d\_signature_{ij}$, а период актуальности описания данного пользователя не завершен.

С учетом модели IT-сервиса (2.26) предикат $P_{serv_{d_i}}$, определяющий IT-сервисы ИС, имеющие право изменять НД d_i за период актуальности данного НД, предложено детализированно описать следующим выражением:

$$P_{serv_{d_i}} = \left(\langle n_i^1, T_i^1 \rangle, \dots, \langle n_i^x, T_i^x \rangle, \dots \langle n_i^N, T_i^N \rangle, \bigcup_{j,p} \langle n_{ijp}^t, T_{ijp}^t \rangle \right). \quad (2.28)$$

Предикат (2.28) позволяет выделить только те IT-сервисы, по результатам функционирования которых состав или содержание НД d_i будут изменены и переданы для использования другим сервисам (в том числе – служебному сервису по взаимодействию с централизованной БД, если таковая реализована в ИС). Предикат (2.28) будет истинным при условии, что описание хотя бы

одного выходного сообщения IT-сервиса, изменяющего НД d_i на протяжении периода актуальности данного НД d_i $[\tau_{bi}, \tau_{ei}]$, совпадут с описаниями данного НД в БНД, а период актуальности описания данного IT-сервиса не окончен.

Выражения (2.27) и (2.28) позволяют разработать метод решения подзадачи определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия. Данный метод представляет собой последовательность таких этапов [98, p. 21].

Этап 1. Определить значение $service\_key_i$ IT-сервиса, для которого предикат $P_{serv_{d_i}} = \left(\langle n_i^1, T_i^1\rangle, \dots, \langle n_i^x, T_i^x\rangle, \dots \langle n_i^N, T_i^N\rangle, \cup_{j,p}\langle n_{ijp}^t, T_{ijp}^t\rangle\right) = 1$. Если предикат будет ложным для всех НД d_i, изменение которых осуществляется в ИС, то сообщить о попытке несанкционированного изменения БНД и завершить применение метода.

Этап 2. Идентифицировать пользователя, работающего с IT-сервисом, значение $service\_key_i$ которого определено на Этапе 1. Если идентификация средствами ИС невозможна, то сообщить о попытке несанкционированного изменения БНД и завершить применение метода.

Этап 3. Определить сигнатуру $d\_signature_{ij}$ пользователя, идентифицированного на Этапе 2.

Этап 4. Если $P_{user_{d_i}} = \left(n_i, d_{signature_{ij}}\right) = 1$, то признать право на модификацию НД d_i пользователя, идентифицированного на Этапе 2, и завершить выполнение метода. В противном случае отказать в праве на модификацию НД d_i пользователю, идентифицированному на Этапе 2, сообщить о попытке несанкционированного изменения БНД пользователем, сигнатура которого определена на Этапе 3, и завершить применение метода.

Разработанные модели определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия, в виде детализированных описаний предикатов $P_{user_{d_i}}$ и $P_{serv_{d_i}}$ выражениями (2.27) и (2.28) и метод определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия, позволяют автоматизировать процесс проверки несанкционированного доступа субъектов ИС к любому НД d_i, описанному моделью (2.4)-(2.6), в рамках действующей на предприятии БНД, представленной в виде выражения (2.8).

2.4 Разработка моделей и метода определения достоверности базы нормативных документов

Для обеспечения достоверности состава, содержания и взаимодействия НД d_i с другими НД, входящими в БНД предприятия, необходимо, чтобы:

а) описания и содержание любого НД d_i создавались, модифицировались или удалялись только теми субъектами ИС, которые имеют на это право;

б) права субъектов ИС, которые осуществляют над описаниями и содержанием НД d_i, были актуальны.

Для проверки этих условий используем предложенные в подразделе 2.2 и подразделе 2.3 модели НД (2.4)-(2.6), БНД (2.8), пользователей ИС (2.18) и IT-сервиса ИС (2.26). На основе этих моделей предложено детализированно описать предикат $P_{acc\_cons_{d_i}}$, определяющий достоверность состава НД d_i за период актуальности данного НД, следующим выражением:

$$P_{acc\_cons_{d_i}} = (n_i^1, \dots, n_i^x, \dots, n_i^N, \tau_{bi}, \tau_{ei}, \tau_{bij}, \tau_{eij}, \tau_{bs_i}, \tau_{es_i}). \quad (2.29)$$

Предикат (2.29) определяет множество атрибутов НД d_i, введенных в описание состава данного НД пользователями ИС и IT-сервисами ИС, имеющими на это право. Предикат (2.29) будет истинным, если будет истинной следующая система условий:

$$\begin{cases} \langle n_i, \{n_i^x\}\rangle \wedge \cup_i \left\langle n_i, \left\{\left\langle n_i^x, T_i^x \right\rangle\right\}, \left(R_{d_k}^{d_i}\right), \left(\varphi_{d_k}^{d_i}\right)\right\rangle; \\ \tau_{bi} \neq \emptyset \wedge \tau_{ei} = \emptyset; \\ \tau_{bij} \neq \emptyset \wedge \tau_{eij} = \emptyset; \\ \tau_{bs_i} \neq \emptyset \wedge \tau_{es_i} = \emptyset. \end{cases} \quad (2.30)$$

Система условий (2.30):

а) проверяет наличие описания состава НД d_i в БНД предприятия;

б) запрещает менять исторические версии описаний состава НД d_i;

в) запрещает менять описания состава НД d_i в БНД предприятия пользователю ИС, не имеющему актуальных прав;

г) запрещает менять описания состава НД d_i в БНД предприятия IT-сервису ИС, не имеющему актуальных прав.

Предикат $P_{acc\_cont_{d_i}}$, определяющий достоверность содержания НД d_i за период актуальности данного НД, с использованием моделей (2.4)-(2.6), (2.8), (2.18) и (2.26) предлагается детализированно описать следующим образом:

$$P_{acc\_cont_{d_i}} = \left(\langle n_i^1, T_i^1\rangle, \dots, \langle n_i^x, T_i^x\rangle, \dots \langle n_i^N, T_i^N\rangle, \tau_{bi}, \tau_{ei}, \tau_{bij}, \tau_{eij}, \tau_{bs_i}, \tau_{es_i}\right). \quad (2.31)$$

Предикат (2.31) определяет множество значений атрибутов НД d_i, имеющих соответствующий тип данных и введенных в описание состава данного НД пользователями ИС и IT-сервисами ИС, имеющими на это право.

Предикат (2.31) будет истинным, если будет истинной следующая система условий:

$$\begin{cases} \langle n_i, \{\langle n_i^x, T_i^x \rangle\} \rangle \wedge \cup_i \left\langle n_i, \left\{ \left\langle n_i^x, T_i^x \right\rangle \right\}, \left(R_{d_k}^{d_i} \right), \left(\varphi_{d_k}^{d_i} \right) \right\rangle; \\ \tau_{bi} \neq \emptyset \wedge \tau_{ei} = \emptyset; \\ \tau_{bij} \neq \emptyset \wedge \tau_{eij} = \emptyset; \\ \tau_{bs_i} \neq \emptyset \wedge \tau_{es_i} = \emptyset. \end{cases} \quad (2.32)$$

Система условий (2.32):

а) проверяет наличие описания содержания НД d_i в БНД предприятия;

б) запрещает менять исторические версии описаний содержания НД d_i;

в) запрещает менять описания содержания НД d_i в БНД предприятия пользователю ИС, не имеющему актуальных прав;

г) запрещает менять описания содержания НД d_i в БНД предприятия IT-сервису ИС, не имеющему актуальных прав.

Предикат $P_{acc\_inter_{d_i}}$, определяющий достоверность взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД, с использованием моделей (2.4)-(2.6), (2.8), (2.18) и (2.26) предлагается разделить на два предиката (по аналогии с предикатами (2.12) и (2.14)):

а) предикат $P_{acc\_R_{d_i}}$, определяющий достоверность взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД;

б) предикат $P_{acc\_\varphi_{d_i}}$, определяющий достоверность описывающий факт тождественности описаний НД d_i и НД d_k в БРН предприятия за период актуальности данного НД d_i.

Предикат $P_{acc\_R_{d_i}}$ предлагается детализированно описать следующим образом:

$$P_{R_{d_i}} = \left(P_{R_{d_1}^{d_i}}, \dots, P_{R_{d_k}^{d_i}}, \dots, P_{R_{d_N}^{d_i}}, \tau_{bi}, \tau_{ei}, \tau_{bij}, \tau_{eij}, \tau_{bs_i}, \tau_{es_i} \right)_{i \neq k}. \quad (2.33)$$

Предикат (2.33) определяет множество описаний связей между НД d_i и НД d_k, введенных в описание данного НД пользователями ИС и IT-сервисами ИС, имеющими на это право.

Предикат (2.33) будет истинным, если будет истинной следующая система условий:

$$\begin{cases} \langle n_i, \left(R_{d_k}^{d_i} \right) \rangle \wedge \cup_i \left\langle n_i, \left\{ \left\langle n_i^x, T_i^x \right\rangle \right\}, \left(R_{d_k}^{d_i} \right), \left(\varphi_{d_k}^{d_i} \right) \right\rangle; \\ \tau_{bi} \neq \emptyset \wedge \tau_{ei} = \emptyset; \\ \tau_{bij} \neq \emptyset \wedge \tau_{eij} = \emptyset; \\ \tau_{bs_i} \neq \emptyset \wedge \tau_{es_i} = \emptyset. \end{cases} \quad (2.34)$$

Система условий (2.34):

а) проверяет наличие описания связи между НД d_i и НД d_k в БНД предприятия;

б) запрещает менять исторические версии описаний связи между НД d_i и НД d_k;

в) запрещает менять описания связи между НД d_i и НД d_k в БНД предприятия пользователю ИС, не имеющему актуальных прав;

г) запрещает менять описания связи между НД d_i и НД d_k в БНД предприятия IT-сервису ИС, не имеющему актуальных прав.

Предикат $P_{acc\_\varphi_{d_i}}$ предлагается детализированно описать следующим образом:

$$P_{acc\_\varphi_{d_i}} = \left(P_{\varphi_{d_1}^{d_i}}, \dots, P_{\varphi_{d_k}^{d_i}}, \dots, P_{\varphi_{d_N}^{d_i}}, \tau_{bi}, \tau_{ei}, \tau_{bij}, \tau_{eij}, \tau_{bs_i}, \tau_{es_i} \right)_{i \neq k}. \quad (2.35)$$

Предикат (2.35) определяет множество тождественности описаний НД d_i и НД d_k, образующими БНД предприятия, введенных в описание пользователями ИС и IT-сервисами ИС, имеющими на это право.

Предикат (2.35) будет истинным, если будет истинной следующая система условий:

$$\begin{cases} \langle n_i, \left(\varphi_{d_k}^{d_i}\right)\rangle \wedge \cup_i \left\langle n_i, \left\{\left\langle n_i^x, T_i^x \right\rangle\right\}, \left(R_{d_k}^{d_i}\right), \left(\varphi_{d_k}^{d_i}\right)\right\rangle; \\ \tau_{bi} \neq \emptyset \wedge \tau_{ei} = \emptyset; \\ \tau_{bij} \neq \emptyset \wedge \tau_{eij} = \emptyset; \\ \tau_{bs_i} \neq \emptyset \wedge \tau_{es_i} = \emptyset. \end{cases} \quad (2.36)$$

Система условий (2.36):

а) проверяет наличие описания факта тождественности связи между НД d_i и НД d_k в БНД предприятия;

б) запрещает менять исторические версии описаний фактов тождественности связи между НД d_i и НД d_k;

в) запрещает менять описания факта тождественности связи между НД d_i и НД d_k в БНД предприятия пользователю ИС, не имеющему актуальных прав;

г) запрещает менять описания факта тождественности связи между НД d_i и НД d_k в БНД предприятия IT-сервису ИС, не имеющему актуальных прав.

Выражения (2.29)-(2.36) позволяют разработать метод решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД в рамках БНД предприятия. Данный метод представляет собой последовательность таких этапов.

Этап 1. Выбрать НД d_i и выполнить логическую операцию (2.16). Если операция (2.16) принимает значение «истина», то перейти к Этапу 2. В

противном случае сообщить об отсутствии описания НД d_i в БНД предприятия и завершить применение метода.

Этап 2. Если для выбранного на Этапе 1 НД d_i $P_{acc\_cons_{d_i}} = (n_i^1, \dots, n_i^x, \dots, n_i^N, \tau_{bi}, \tau_{ei}, \tau_{bij}, \tau_{eij}, \tau_{bs_i}, \tau_{es_i}) = 1$, то перейти к Этапу 3. В противном случае сообщить о нарушении достоверности описания состава НД d_i в БНД предприятия и завершить применение метода.

Этап 3. Если для выбранного на Этапе 1 НД d_i $P_{acc\_cont_{d_i}} = \left(\langle n_i^1, T_i^1\rangle, \dots, \langle n_i^x, T_i^x\rangle, \dots \langle n_i^N, T_i^N\rangle, \tau_{bi}, \tau_{ei}, \tau_{bij}, \tau_{eij}, \tau_{bs_i}, \tau_{es_i}\right) = 1$, то перейти к Этапу 4. В противном случае сообщить о нарушении достоверности описания возможного содержания НД d_i в БНД предприятия и завершить применение метода.

Этап 4. Если для выбранного на Этапе 1 НД d_i $P_{R_{d_i}} = \left(P_{R_{d_1}^{d_i}}, \dots, P_{R_{d_k}^{d_i}}, \dots, P_{R_{d_N}^{d_i}}, \tau_{bi}, \tau_{ei}, \tau_{bij}, \tau_{eij}, \tau_{bs_i}, \tau_{es_i}\right)_{i \neq k} = 1$, то перейти к Этапу 5. В противном случае сообщить о нарушении достоверности описаний взаимодействия НД d_i с конкретными НД d_k в БНД предприятия и завершить применение метода.

Этап 5. Для выбранного на Этапе 1 НД d_i выполнить логическую операцию

$$P_{acc\_\varphi_{d_i}} = 1 \vee \varphi_{d_k}^{d_i} = \emptyset. \quad (2.37)$$

Если операция (2.37) принимает значение «истина», то сообщить об успешном обеспечении достоверности НД d_i и завершить применение метода. В противном случае сообщить о нарушении достоверности тождественности описаний НД d_i и описаний конкретных НД d_k в БНД предприятия и завершить применение метода.

Разработанные модели обеспечения достоверности БНД предприятия в виде детализированных описаний предикатов $P_{acc\_cons_{d_i}}$, $P_{acc\_cont_{d_i}}$ и $P_{acc\_inter_{d_i}}$ выражениями (2.29), (2.31), (2.33) и (2.35) и метод обеспечения достоверности БНД предприятия позволяют автоматизировать процесс проверки достоверности состава, содержания и взаимодействия любого НД d_i, описанного моделью (2.4)-(2.6), в рамках действующей на предприятии БНД, представленной в виде выражения (2.8).

Выводы ко второму разделу

1. Для достижения поставленной цели исследования была разработана общая постановка задачи обеспечения целостности БНД предприятия. Данная задача представлена выражениями (2.2) и (2.3) в виде системы предикатов. Предложено считать БНД целостной, если для каждого НД d_i все предикаты системы (2.3) будут истинными.

2. Предложено разделить задачу обеспечения целостности на подзадачи обеспечения неизменности и достоверности состава, содержания и взаимодействия любого НД d_i, в рамках действующей на предприятии БНД, а также подзадачу определения субъектов ИС, имеющих право на изменение состава, содержания и взаимодействия любого НД d_i, в рамках действующей на предприятии БНД.

3. Для детализированных описаний предикатных моделей и метода обеспечения неизменности состава, содержания и взаимодействия любого НД d_i, в рамках действующей на предприятии БНД были разработаны модели НД (2.4)-(2.6) и БНД (2.8). На основе этих моделей были разработаны предикатные модели (2.9), (2.10), (2.12) и (2.14), а также метод обеспечения неизменности БНД предприятия. Полученные результаты позволяют автоматизировать процесс проверки неизменности состава, содержания и взаимодействия любого НД d_i, описанного моделью (2.4)-(2.6), в рамках действующей на предприятии БНД, представленной в виде выражения (2.8).

4. Для детализированных описаний предикатных моделей и метода обеспечения определения субъектов ИС, имеющих право на изменение состава, содержания и взаимодействия любого НД d_i, в рамках действующей на предприятии БНД были разработаны модели пользователя ИС (2.18) и IT-сервиса ИС (2.26). На основе этих моделей были разработаны предикатные модели (2.21), (2.27) и (2.28), а также метод решения подзадачи определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия. Полученные результаты позволяют автоматизировать процесс проверки неизменности состава, содержания и взаимодействия любого НД d_i, описанного моделью (2.4)-(2.6), в рамках действующей на предприятии БНД, представленной в виде выражения (2.8).

5. Для детализированных описаний предикатных моделей и метода обеспечения достоверности состава, содержания и взаимодействия любого НД d_i, в рамках действующей на предприятии БНД были использованы ранее разработанные модели НД (2.4)-(2.6), БНД (2.8), пользователя ИС (2.18) и IT-сервиса ИС (2.26). На основе этих моделей были разработаны предикатные модели (2.29), (2.31), (2.33) и (2.35), а также метод обеспечения достоверности БНД предприятия. Полученные результаты позволяют автоматизировать процесс проверки достоверности состава, содержания и взаимодействия любого НД d_i, описанного моделью (2.4)-(2.6), в рамках действующей на предприятии БНД, представленной в виде выражения (2.8).

Основные результаты данного раздела изложены в работе [98, p. 15-22].

3 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ БАЗЫ НОРМАТИВНЫХ ДОКУМЕНТОВ ПРЕДПРИЯТИЯ

3.1 Разработка информационной технологии обеспечения целостности базы нормативных документов предприятия

Для проверки работоспособности приведенных моделей и методов, прежде чем разрабатывать модель информационно-аналитической системы, на примере Департамента приема НАО "Северо-Казахстанский университет им. М. Козыбаева" сформирована модель бизнес-процесса приема документов у абитуриентов. Модель, построенная на основе бизнес-логики процесса с наложением требований нормативной документации, приведена на рисунке 3.1.

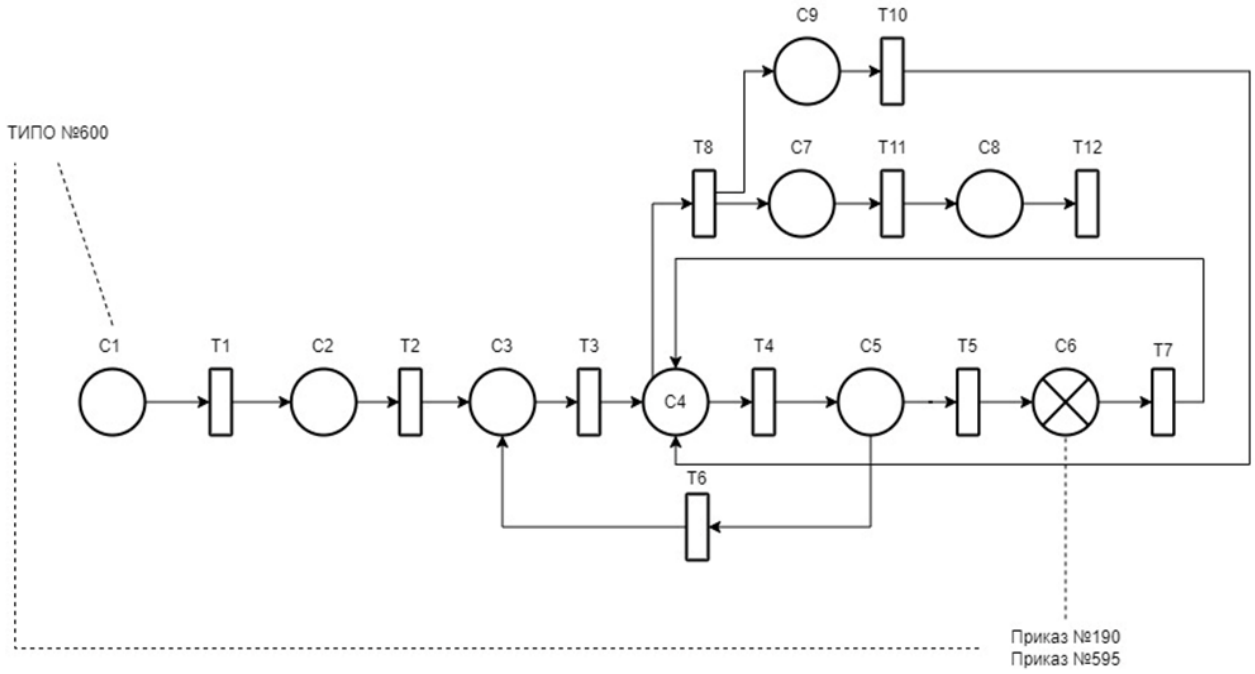

Рисунок 3.1 – Модель бизнес-процесса приема документов

В приведенной модели принятые обозначения семантически определяют следующие этапы (состояния и переходы):

– заявления поступают в систему (C1);
– регистрация (C2);
– подача заявления (C3);
– заявление в системе и базе данных (C4);
– заявление, обработка заявления (C5);
– проверка документов (C6);
– проект приказа (C7);
– приказ (C8);
– отказ (C9);
– регистрация заявления (T1);
– подача заявления (T2);

– обработка заявления (Т3);
– отправка техническому секретарю (Т4);
– проверка заполнения полей (Т5);
– отправка на доработку (Т6);
– проверка документов (Т7);
– соответствие документов (Т8);
– отправка на проект приказа (Т9);
– отправка отказа (Т10);
– утверждение проекта приказа (Т11);
– запуск приказа (Т12).

В процессе импульсного моделирования по построенной схеме обнаружено нарушение непротиворечивости, вызванное несогласованностью документов - Приказ №190 и Приказ №595. Далее, отрегулировав выявленные противоречия, моделирование прошло без коллизий и позволило сформировать целостную базу нормативных документов и сопровождать бизнес-процессы с соблюдением условия контроля целостности базы нормативных документов.

Впоследствии, при использовании моделей и методов, разработанных в разделе 2, нарушений целостности не происходило, что позволяет утверждать, что построенная на основе этих моделей и методов система позволяет осуществлять контроль целостности базы нормативных документов.

Разработанные в разделе 2 модели и методы решения задачи обеспечения целостности БНД предприятия определяют основные особенности разработки информационной технологии обеспечения целостности БНД. Под информационной технологией в [106] предлагается понимать приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных. Следовательно, для описания информационной технологии обеспечения целостности БНД предприятия, необходимо:

а) описать взаимодействие этой информационной технологии с другими элементами СУП;

б) описать функции этой информационной технологии;

в) описать структуры данных, которые собираются, обрабатываются, передаются и используются этой информационной технологией;

г) описать алгоритмы решения отдельных подзадач обеспечения целостности БНД предприятия средствами вычислительной техники в рамках этой информационной технологии.

Для описания взаимодействия информационной технологии обеспечения целостности БНД предприятия с другими элементами СУП предлагается использовать контекстную диаграмму потоков данных (Data Flow Diagram, DFD). Данный вид диаграмм описывает информационную технологию как работу, с которой взаимодействуют другие элементы СУП, представленные в виде внешних сущностей [107].

Контекстная диаграмма информационной технологии обеспечения целостности БНД предприятия имеет вид, представленный на рисунке 3.2.

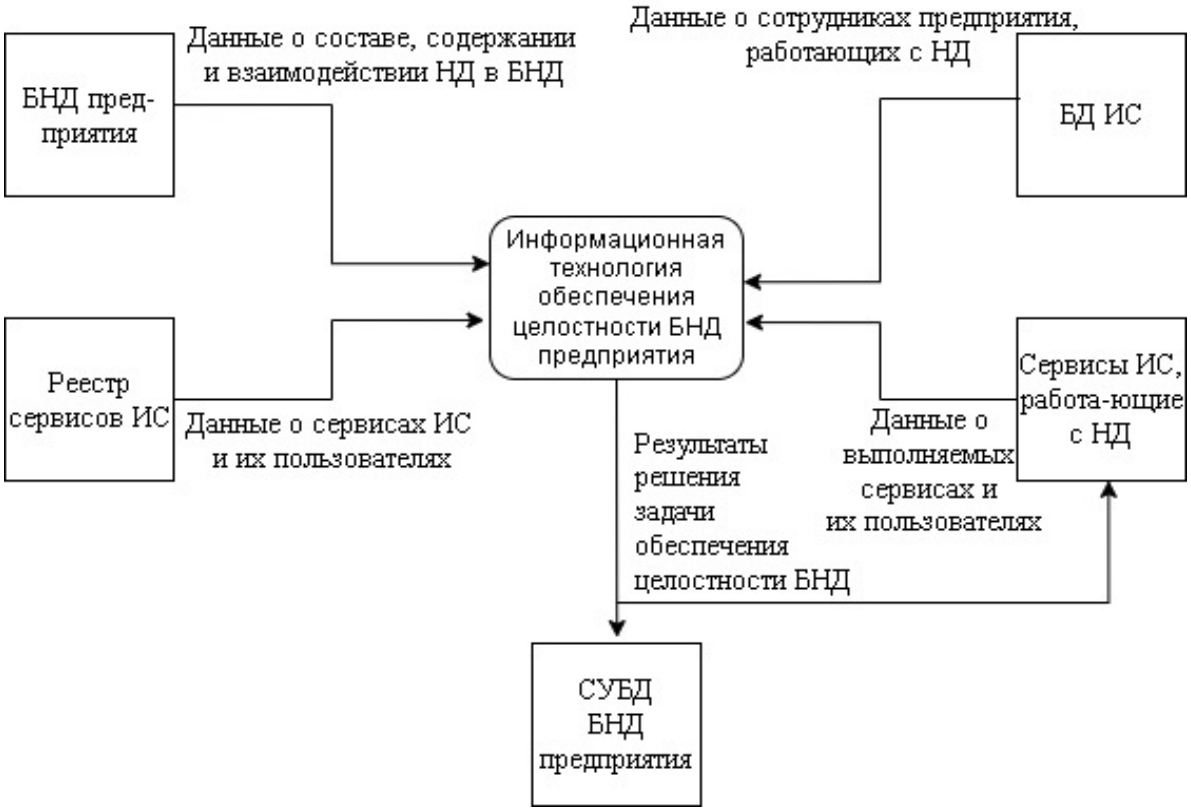

Рисунок 3.2 – Контекстная диаграмма потоков данных информационной технологии обеспечения целостности базы нормативных документов предприятия

Здесь и в дальнейшем для визуального представления DFD использована нотация Гейна-Сарсона [107, с. 122].

Основными входными данными информационной технологии обеспечения целостности БНД предприятия являются:

– данные о составе, содержании и взаимодействии НД в БНД, которые выбираются из таблиц БНД предприятия и используются информационной технологией для определения предикатов $P_{cons_{d_i}}$, $P_{cont_{d_i}}$ и $P_{inter_{d_i}}$, предикатов $P_{user_{d_i}}$ и $P_{serv_{d_i}}$, а также предикатов $P_{acc\_cons_{d_i}}$, $P_{acc\_cont_{d_i}}$ и $P_{acc\_inter_{d_i}}$;

– данные о сервисах ИС и их пользователях, которые выбираются из реестра сервисов ИС управления предприятием и используются информационной технологией для определения предикатов $P_{user_{d_i}}$ и $P_{serv_{d_i}}$, а также предикатов $P_{acc\_cons_{d_i}}$, $P_{acc\_cont_{d_i}}$ и $P_{acc\_inter_{d_i}}$;

– данные о сотрудниках предприятия, работающих с НД, которые выбираются из таблиц БД ИС управления предприятием (при условии эксплуатации в рамках ИС функционального модуля или сервисов, автоматизирующих решение задач управления кадрами) и используются информационной технологией для определения предиката $P_{user_{d_i}}$;

– данные о выполняемых сервисах и их пользователях, которые направляются в информационную технологию от сервисов ИС управления

предприятием, выполняемых в ходе решения задачи обеспечения целостности БНД, в рамках которых выполняются операции над НД или их элементами, и используются информационной технологией для определения предикатов $P_{user_{d_i}}$ и $P_{serv_{d_i}}$, а также предикатов $P_{acc\_cons_{d_i}}$, $P_{acc\_cont_{d_i}}$ и $P_{acc\_inter_{d_i}}$.

Основными выходными данными информационной технологии обеспечения целостности БНД предприятия являются результаты решения задачи обеспечения целостности БНД предприятия. Эти результаты представлены сигналом, который может принимать один из следующих видов:

а) сигнал, содержащий код успешного решения задачи обеспечения целостности БНД предприятия;

б) сигнал, содержащий код ошибки, выявленной в ходе решения задачи обеспечения целостности БНД предприятия;

в) сигнал, содержащий код чрезвычайного завершения применения информационной технологии до окончания решения задачи обеспечения целостности БНД предприятия.

Получателями этого сигнала предполагаются СУБД, в рамках которой предусматривается эксплуатация БНД предприятия, а также сервисы ИС управления предприятиями, выполняемые в ходе решения задачи обеспечения целостности БНД, которые выполняют операции над НД и их элементами. В случае получения сигналов, содержащих код ошибки или код чрезвычайного завершения применения разрабатываемой информационной технологии, СУБД выполнит откат текущей транзакции над данными НД, а сервисы начнут формирование выходного сообщения пользователю, в котором будет указана причина невозможности выполнения операции над обрабатываемым НД.

Для описания функций информационной технологии обеспечения целостности БНД предприятия предлагается использовать диаграмму декомпозиции первого уровня DFD. На этой диаграмме функции показаны в виде работ DFD, взаимодействие которых осуществляется в виде потоков данных (показаны стрелками).

Диаграмма декомпозиции первого уровня информационной технологии обеспечения целостности БНД предприятия имеет вид, представленный на рисунке 3.3.

Предложенное на рисунке 3.3 описание взаимодействия функций информационной технологии обеспечения целостности БНД предприятия позволяет:

а) отказаться от выполнения функций решения подзадач обеспечения достоверности и неизменности состава, содержания и взаимодействия НД в случае выявления ошибки в ходе выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава, содержания и взаимодействия НД;

б) отказаться от выполнения функции решения подзадачи обеспечения неизменности состава, содержания и взаимодействия НД в случае выявления ошибки в ходе выполнения функции решения подзадачи обеспечения достоверности состава, содержания и взаимодействия НД.

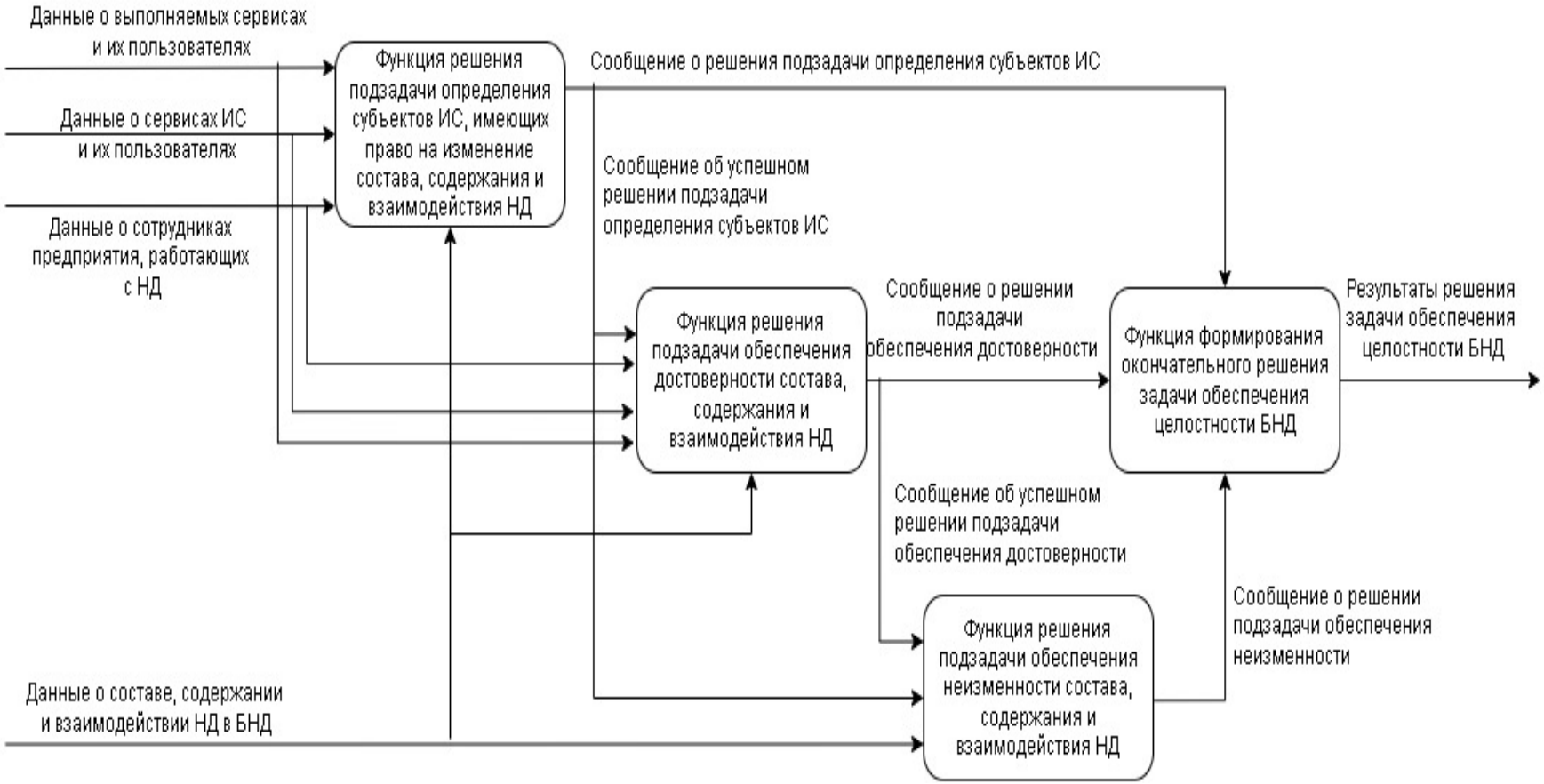

Рисунок 3.3 – Диаграмма декомпозиции первого уровня диаграммы потоков данных информационной технологии обеспечения целостности базы нормативных документов предприятия

Такая организация взаимодействия позволяет уменьшить вычислительную нагрузку на средства вычислительной техники при попытках несанкционированного изменения состава, содержания и взаимодействия НД в БНД предприятия.

Для описания применения разработанных в разделе 2 моделей и методов решения задачи обеспечения целостности БНД предприятия в рамках разработанной информационной технологии обеспечения целостности БНД предприятия предлагается использовать диаграмму SwimLane. Данная диаграмма является разновидностью диаграммы IDEF3, позволяющей явно описать роли и ответственности исполнителей в конкретной технологической операции [107, с. 124]. В нашем случае использование диаграммы SwimLane позволит явно описать принадлежность разработанных в разделе 2 моделей и методов к конкретным функциям информационной технологии, последовательность выполнения операций информационной технологии и логику взаимодействия потоков объектов между операциями информационной технологии.

Диаграмма SwimLane информационной технологии обеспечения целостности БНД предприятия приведена на рисунке 3.4.

На рисунке 3.4 приняты следующие обозначения:

– литерой «A» обозначен поток под названием «Сообщение об ошибочном решении подзадачи определения субъектов ИС»;

– литерой «B» обозначен поток под названием «Сообщение об ошибочном решении подзадачи определения достоверности состава, содержания и взаимодействия НД»;

– литерой «C» обозначен поток под названием «Сообщение об успешном решении подзадачи определения достоверности состава, содержания и взаимодействия НД»;

– литерой «D» обозначен поток под названием «Сообщение о решении подзадачи определения достоверности состава, содержания и взаимодействия НД»;

– литерой «E» обозначен поток под названием «Сообщение об ошибочном решении подзадачи определения неизменности состава, содержания и взаимодействия НД»;

– литерой «F» обозначен поток под названием «Сообщение об успешном решении подзадачи определения неизменности состава, содержания и взаимодействия НД».

Для описания структур данных, которые собираются, обрабатываются, передаются и используются информационной технологией обеспечения целостности БНД предприятия, предлагается использовать диаграмму «сущность - связь». Эта диаграмма описывает концептуальную модель данных разрабатываемой информационной технологии и позволяет визуализировать основные сущности и атрибуты, которые следует использовать в ходе разработки алгоритмов выполнения функций данной технологии.

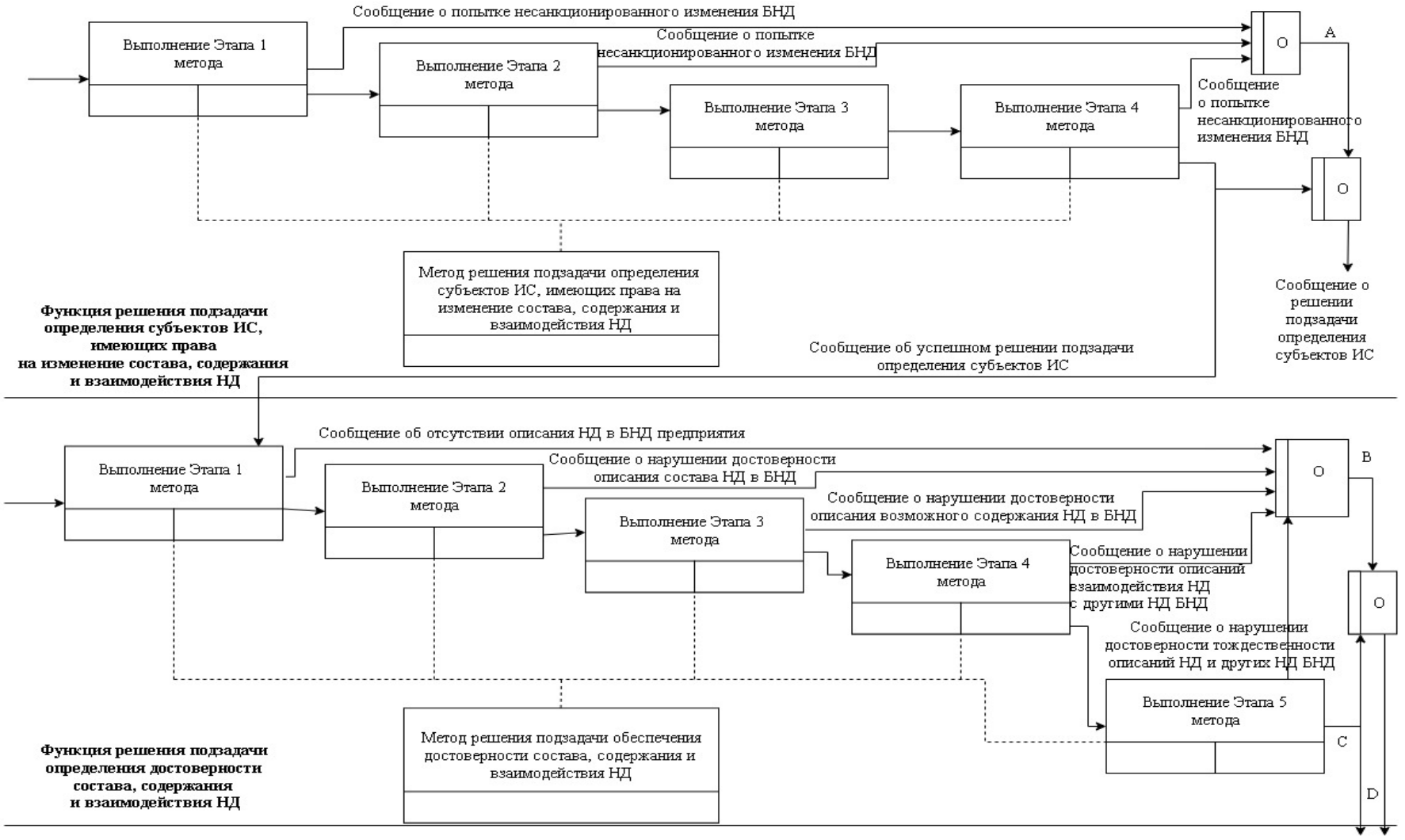

Рисунок 3.4 – Диаграмма SwimLane информационной технологии обеспечения целостности базы нормативных документов предприятия, лист 1

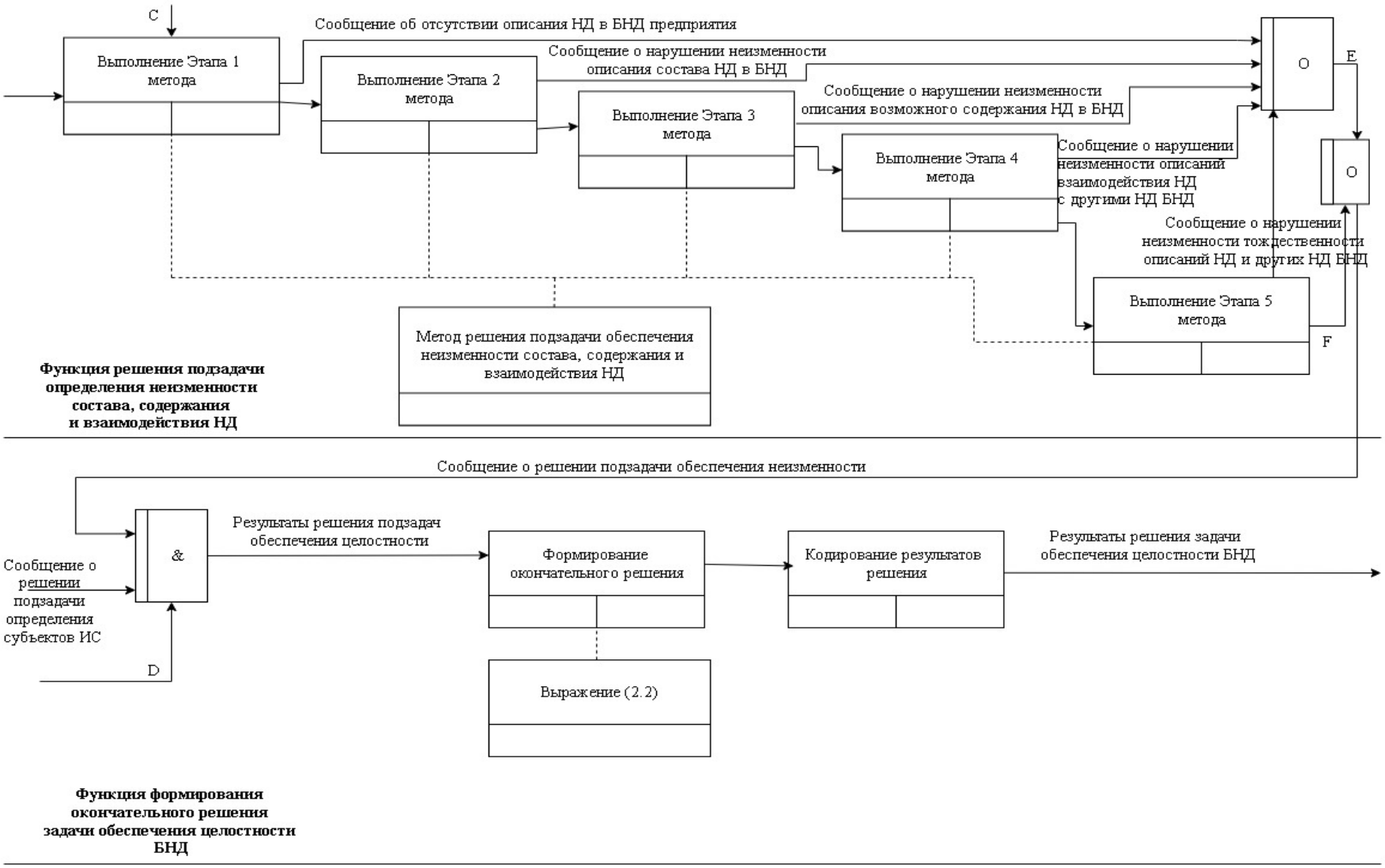

Рисунок 3.4, лист 2

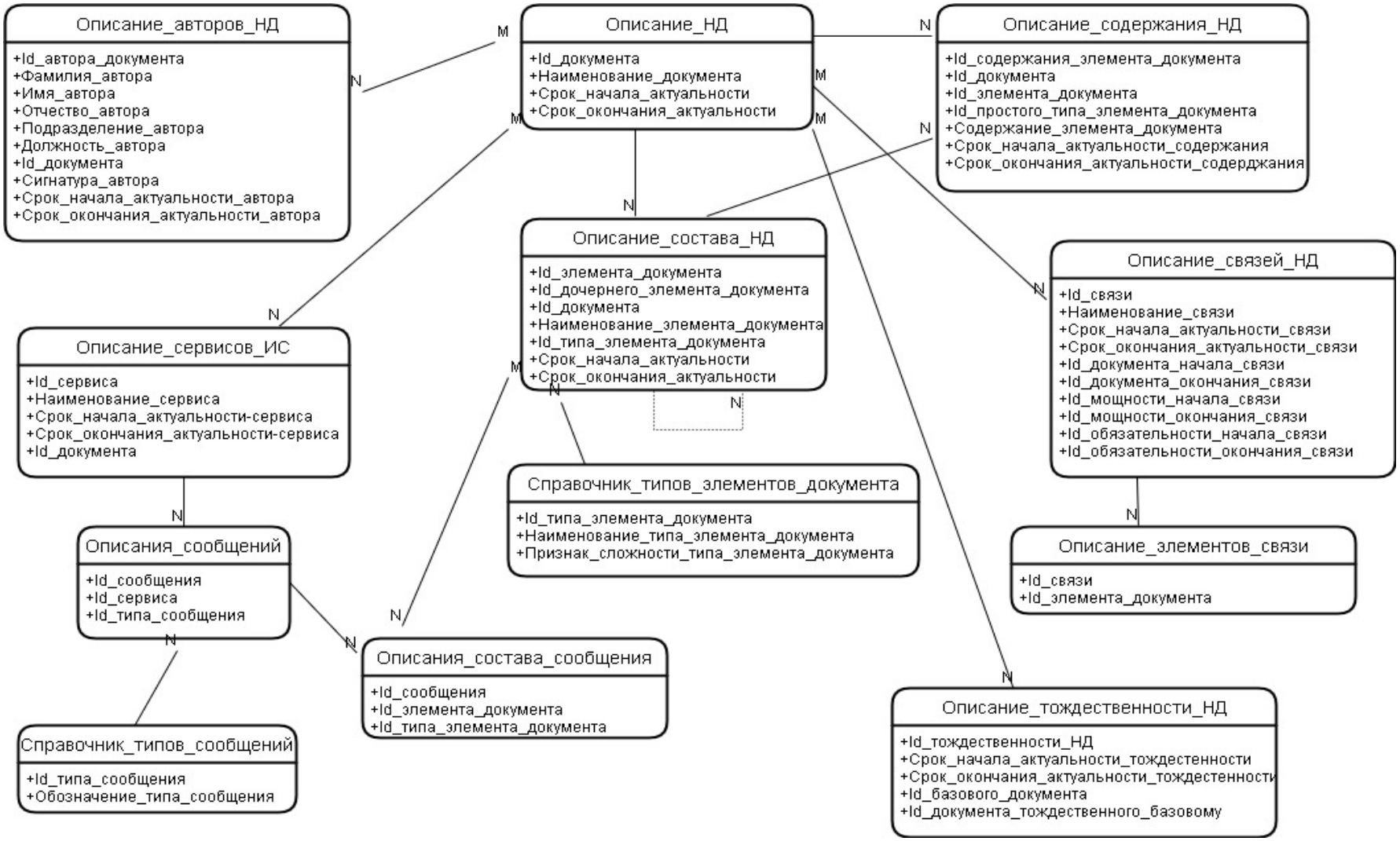

Рисунок 3.5 – Фрагмент концептуальной модели данных информационной технологии обеспечения целостности базы нормативных документов предприятия

В соответствии с рисунком 3.5, приведен фрагмент концептуальной модели данных информационной технологии обеспечения целостности БНД предприятия.

На рисунке 3.5 показаны только те сущности, атрибуты и связи, которые являются основой для дальнейших детальных описаний алгоритмов выполнения отдельных функций данной технологии.

Следует отметить, что разработанные визуальные модели информационной технологии обеспечения целостности БНД предприятия, показанные на рисунках 3.2, 3.33, 3.4, 3.5, являются платформонезависимыми. Это позволяет в дальнейшем реализовать разработанную информационную технологию обеспечения целостности БНД предприятия для различных СУБД и комплексов технических средств, которые могут использоваться в ИС управления различными предприятиями.

3.2 Разработка алгоритмов решения подзадачи определения субъектов, имеющих право на изменение базы нормативных документов предприятия

Для детализированного описания сценария выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава содержания и взаимодействия НД, предлагается использовать диаграммы деятельности (Activity Diagram) языка объектно-ориентированного визуального моделирования UML. Выбор данного вида диаграмм обусловлен рекомендациями, изложенными в [108]. Данные диаграммы позволяют представить схему алгоритма в виде набора деятельностей (activities) и логических элементов, определяющих условия и порядок выполнения деятельностей. Под деятельностью для платформо-независимых концептуальных описаний алгоритмов выполнения функций информационной технологии обеспечения целостности БНД предприятия следует понимать некоторую задачу, которую необходимо выполнить вручную или автоматизированным способом [108, с. 88; 109].

Как показано на рисунке 3.4, в основе алгоритма выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава содержания и взаимодействия НД, лежит алгоритм применения метода решения подзадачи определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия, рассмотренный в подразделе 2.3. Поэтому предлагается рассматривать алгоритм выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава содержания и взаимодействия НД, как совокупность двух следующих частей:

а) обобщенный алгоритм выполнения функции, который описывает действия по сбору данных, необходимых для выполнения функции, передаче собранных данных в алгоритм применения метода, получению результатов выполнения алгоритма применения метода, кодированию этих результатов и передаче их другим функциям информационной технологии;

б) алгоритм применения метода решения подзадачи определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия.

Обобщенный алгоритм выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава содержания и взаимодействия НД, состоит из следующих шагов:

Шаг 1. Переменной *result_function_determine_subjects* присвоить значение 0, переменной *name_result_fds* присвоить значение «Проверка прав начата», переменной *Id_document* присвоить значение 0.

Шаг 2. Сформировать массив *array_service_keys*, который содержит ключи всех сервисов ИС, активных в момент выполнения функции.

Шаг 3. Сформировать массив *array_user_passwords*, который содержит пароли всех пользователей, работающих с сервисами ИС, активными в момент выполнения функции.

Шаг 4. Определить НД d_i, выполнение транзакции над которым завершается и установить значение переменной *Id_document=i*.

Шаг 5. Выполнить алгоритм применения метода решения подзадачи определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия.

Шаг 6. Если алгоритм, выполненный на Шаге 5, завершен успешно, то присвоить переменной *result_function_determine_subjects* значение 1, а переменной *name_result_fds* присвоить значение «Проверка прав выполнена успешно». После этого перейти к Шагу 8.

Шаг 7. Если получено сообщение о попытке несанкционированного изменения БНД, то присвоить переменной *result_function_determine_subjects* значение 0, а переменной *name_result_fds* в зависимости от того, на каком этапе метода была обнаружена ошибка, присвоить одно из следующих значений:

а) значение «Попытка несанкционированного изменения БНД неизвестным сервисом» (ошибка обнаружена в ходе выполнения Этапа 1 метода);

б) значение «Попытка несанкционированного изменения БНД неизвестным пользователем» (ошибка обнаружена в ходе выполнения Этапа 2 метода);

в) значение «Попытка несанкционированного изменения БНД пользователем с сигнатурой $d\_signature_{ij}$» (ошибка обнаружена в ходе выполнения Этапа 4 метода).

Шаг 8. Передать значения переменных *result_function_determine_subjects* и *name_result_fds* в другие функции информационной технологии и завершить выполнение алгоритма.

Диаграмма деятельности обобщенного алгоритма выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава содержания и взаимодействия НД, приведена на рисунке 3.6.

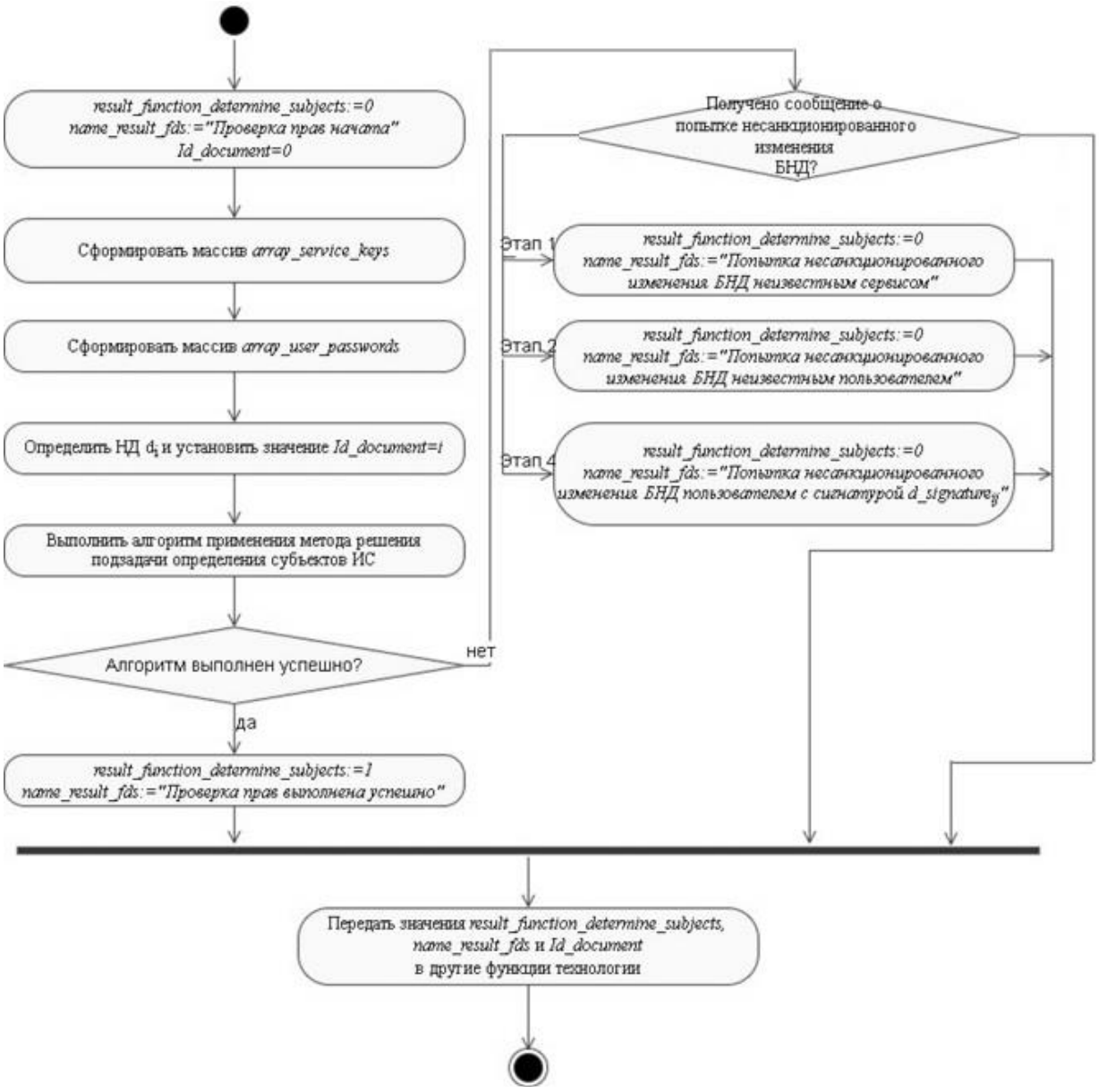

Рисунок 3.6 – Диаграмма деятельности обобщенного алгоритма выполнения функции решения подзадачи определения субъектов информационной системы

Алгоритм применения метода решения подзадачи определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия, состоит из следующих шагов:

Шаг 1. Определить значения переменных $service\_key_i = 0$; *stage_number=0*; *user_password=« »*; *user_surname=« »*; *user_name=« »*; *user_patron=« »*; $d\_signature_{ij} = 0$.

Шаг 2. Для НД d_i определить значение *Описание_НД.Id_документа*.

Шаг 3. Сформировать массив значений *array_doc_elements*, состоящий из кортежей $\langle n_i^1, T_i^1 \rangle, \dots, \langle n_i^x, T_i^x \rangle, \dots \langle n_i^N, T_i^N \rangle$ (значения которых определяются как *<Описание_состава_НД.Наименование_элемента_документа; Справочник_типов_элементов_документа.Наименование_типа_элемента_документа>*), для каждого из которых выполняются условия

Описание_НД.Id_документа=Описание_состава_НД.Id_документа и *Справочник_типов_элементов_документа.Id_типа_элемента_документа= Описание_состава_НД. Id_типа_элемента_документа*.

Шаг 4. Выбрать из реестра сервисов ИС значение $service\_key_i$, для сервиса которого выполняется условие $\left(\langle n_i^1, T_i^1\rangle, \dots, \langle n_i^x, T_i^x\rangle, \dots \langle n_i^N, T_i^N\rangle\right) = (\bigcup_{j,p}\langle n_{ijp}^t, T_{ijp}^t\rangle)$.

Шаг 5. Если $service\_key_i = 0$, то переменной *stage_number* присвоить значение 1 и перейти к Шагу 13.

Шаг 6. Если $service\_key_i \notin array\_service\_keys$, то переменной *stage_number* присвоить значение 1 и перейти к Шагу 13.

Шаг 7. Определить *user_password*∈*array_user_passwords* для $service\_key_i$.

Шаг 8. Найти в служебных таблицах БД ИС значения переменных *user_surname*, *user_name*, *user_patron*, для которых определено значение *user_password*.

Шаг 9. Проверить по содержимому таблиц БД ИС, содержащих кадровые данные, наличие среди сотрудников предприятия пользователя, для которого определены переменные *user_surname*, *user_name*, *user_patron*. Если такого сотрудника нет, то переменной *stage_number* присвоить значение 2 и перейти к Шагу 13.

Шаг 10. Определить значение $d\_signature_{ij}$ пользователя, для которого определены переменные *user_surname*, *user_name*, *user_patron* и выполняется условие *Описание_НД.Id_документа=Описание_авторов_НД.Id_документа*.

Шаг 11. Если $d\_signature_{ij} = 0$, то переменной *stage_number* присвоить значение 4 и перейти к Шагу 13.

Шаг 12. Передать значение переменной *stage_number* в обобщенный алгоритм выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава содержания и взаимодействия НД, и завершить выполнение алгоритма.

Шаг 13. Передать значения переменных *stage_number*, *user_surname*, *user_name*, *user_patron* в обобщенный алгоритм выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава содержания и взаимодействия НД, и завершить выполнение алгоритма.

Диаграмма деятельности алгоритма применения метода решения подзадачи определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия, приведена на рисунке 3.7.

Соответствие шагов алгоритма применения метода решения подзадачи определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия, и этапов метода решения подзадачи определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия, рассмотрено в таблице 3.1.

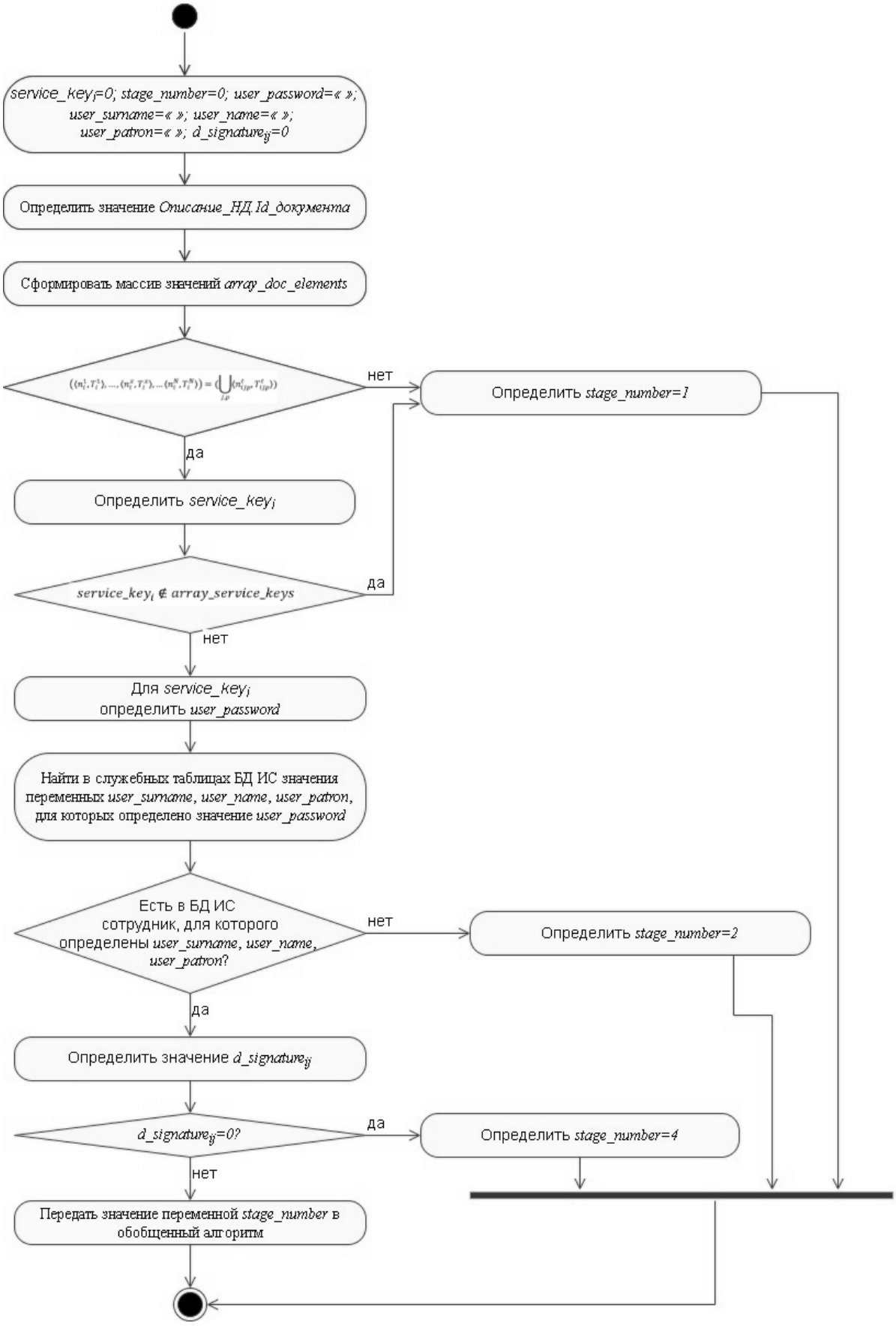

Рисунок 3.7 – Диаграмма деятельности алгоритма применения метода решения подзадачи определения субъектов информационной системы

Таблица 3.1 – Соответствие шагов алгоритма применения метода решения подзадачи определения субъектов информационной системы, имеющих права на изменение состава, содержания и взаимодействия нормативных документов, и этапов данного метода

Шаги алгоритма	Этапы метода
Шаг 1 – Шаг 6	Этап 1
Шаг 7 – Шаг 9	Этап 2
Шаг 10 – Шаг 11	Этап 3
Шаг 12 – Шаг 13	Этап 4

Как уже отмечалось, разработанные алгоритмы описывают платформо-независимый сценарий выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава содержания и взаимодействия НД. Это означает, что в ходе реализации этого сценария данные алгоритмы могут измениться с учетом особенностей платформ, применяемых разработчиками конкретной реализации информационной технологии.

3.3 Разработка алгоритмов решения подзадачи определения достоверности базы нормативных документов

Как показано на рисунке 3.4, в основе алгоритма выполнения функции решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия лежит алгоритм применения метода решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД в рамках БНД предприятия, рассмотренный в подразделе 2.4. Поэтому предлагается рассматривать алгоритм выполнения функции решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия как совокупность двух следующих частей:

а) обобщенный алгоритм выполнения функции, назначение которого аналогично рассмотренному в подразделе 3.2. назначению обобщенного алгоритма выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава содержания и взаимодействия НД;

б) алгоритм применения метода решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД в рамках БНД предприятия.

Обобщенный алгоритм выполнения функции решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия, состоит из следующих шагов:

Шаг 1. Переменной *result_function_determine_authenticity* присвоить значение 0, переменной *name_result_fda* присвоить значение «Проверка достоверности начата».

Шаг 2. Получить значения переменных *result_function_determine_subjects* и *Id_document,* определенные по результатам выполнения функции решения подзадачи определения субъектов ИС, имеющих право на изменение состава содержания и взаимодействия НД.

Шаг 3. Если *result_function_determine_subjects=0,* то переменной *name_result_fda* присвоит значение «Проверка достоверности не проводилась» и перейти на Шаг 7.

Шаг 4. Выполнить алгоритм применения метода решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД в рамках БНД предприятия.

Шаг 5. Если алгоритм, выполненный на Шаге 4, завершен успешно, то присвоить переменной *result_function_determine_ authenticity* значение 1, а переменной *name_result_fda* присвоить значение «Проверка достоверности выполнена успешно». После этого перейти к Шагу 7.

Шаг 6. Если получено сообщение о попытке несанкционированного изменения БНД, то присвоить переменной *result_function_determine_ authenticity* значение 0, а переменной *name_result_fda* в зависимости от того, на каком этапе метода была обнаружена ошибка, присвоить одно из следующих значений:

а) значение «Попытка несанкционированного изменения НД с идентификатором *Id_document*» (ошибка обнаружена в ходе выполнения Этапа 1 метода);

б) значение «Попытка нарушения достоверности описания состава НД d_i в БНД предприятия» (ошибка обнаружена в ходе выполнения Этапа 2 метода);

в) значение «Попытка нарушения достоверности описания возможного содержания НД d_i в БНД предприятия» (ошибка обнаружена в ходе выполнения Этапа 3 метода);

г) значение «Попытка нарушения достоверности описаний взаимодействия НД d_i с конкретными НД d_k в БНД предприятия» (ошибка обнаружена в ходе выполнения Этапа 4 метода);

д) значение «Попытка нарушения достоверности тождественности описаний НД d_i и описаний конкретных НД d_k в БНД предприятия» (ошибка обнаружена в ходе выполнения Этапа 5 метода).

Шаг 7. Передать значения переменных *result_function_determine_authenticity, Id_document* и *name_result_fda* в другие функции информационной технологии и завершить выполнение алгоритма.

Диаграмма деятельности обобщенного алгоритма выполнения функции решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия приведена на рисунке 3.8.

Алгоритм применения метода решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из

БНД предприятия за период актуальности данного НД в рамках БНД предприятия состоит из следующих шагов.

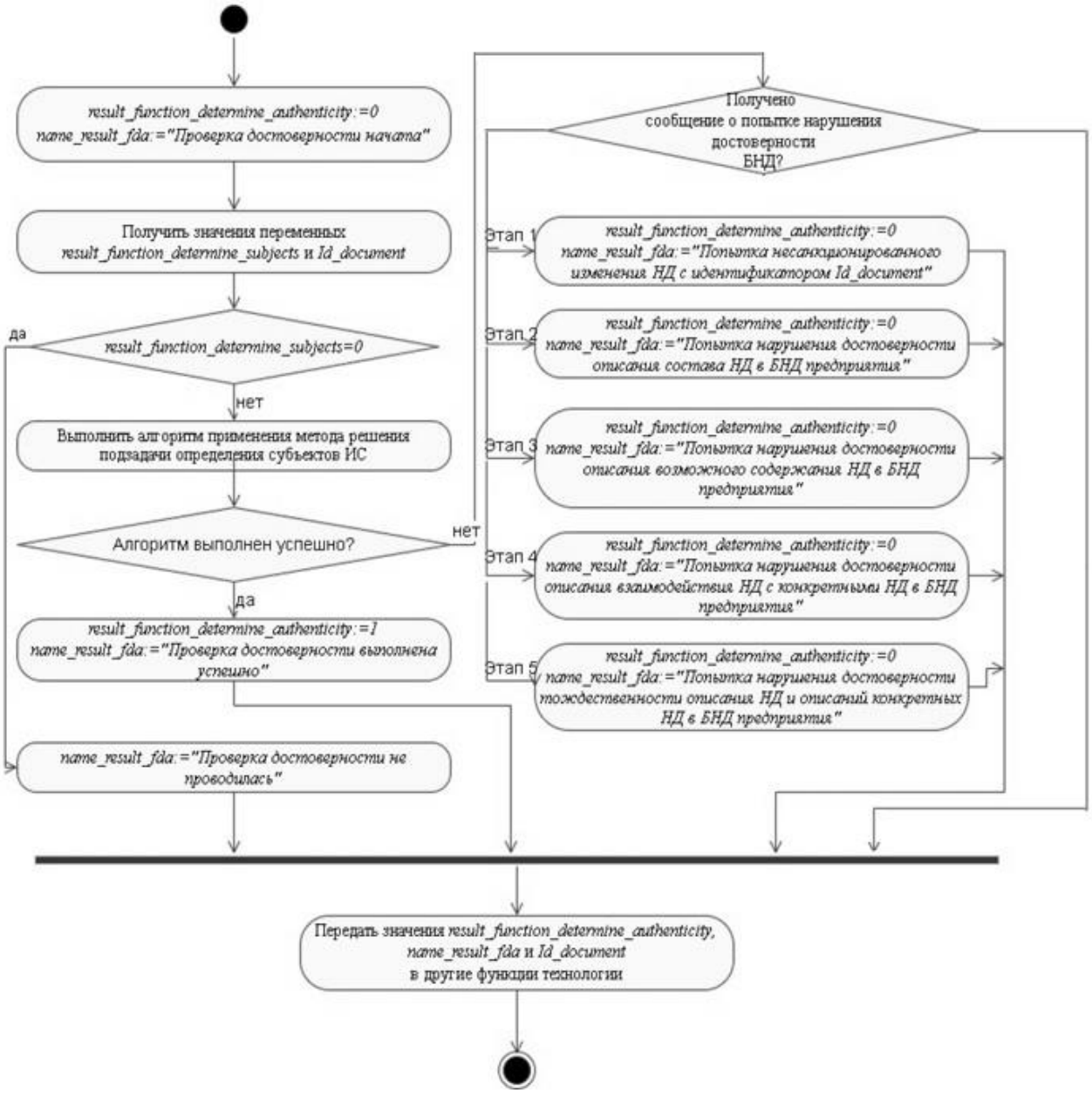

Рисунок 3.8 – Диаграмма деятельности обобщенного алгоритма выполнения функции решения подзадачи определения достоверности состава, содержания и взаимодействия нормативного документа d_i с другими нормативными документами из базы нормативных документов предприятия

Шаг 1. Определить значения переменных *rec_number=0, stage_number=0, time_trans=«».*

Шаг 2. Установить значение переменной *rec_number* как количество записей в БНД, для которых выполняется условие *Описание_НД.Id_документа=Id_document.*

Шаг 3. Если *rec_number=0*, то переменной *stage_number* присвоить значение 1 и перейти к Шагу 19.

Шаг 4. Установить значение переменной *time_trans* как текущую дату и время.

Шаг 5. Сформировать массив записей *array_serv*, для которых справедливо условие *Описание_НД.Id_документа=Описание_сервисов_ИС.Id_документа.*

Шаг 6. Если условие *(array_serv.Срок_начала_актуальности < time_trans) & (array_serv.Срок_окончания_актуальности = «»)* не выполняется, то перейти к Шагу 9.

Шаг 7. Сформировать массив записей *array_cons*, для которых справедливо условие *Описание_НД.Id_документа=Описание_состава_НД.Id_документа.*

Шаг 8. Если в результате выполнения транзакции значения атрибутов массива записей *array_cons* не меняются, то перейти к Шагу 10.

Шаг 9. Принять значение переменной *stage_number=2* и перейти к Шагу 19.

Шаг 10. Сформировать массив записей *array_cont*, для которых справедливо условие *Описание_НД.Id_документа=Описание_содержания_НД.Id_документа.*

Шаг 11. Если в результате выполнения транзакции значения атрибутов массива записей *array_cont* не меняются, то перейти к Шагу 13.

Шаг 12. Принять значение переменной *stage_number=3* и перейти к Шагу 19.

Шаг 13. Сформировать массив записей *array_rel*, для которых справедливо условие (*Описание_НД.Id_документа = Описание_связей_НД.Id_документа_начала_связи) или* (*Описание_НД.Id_документа = Описание_связей_НД.Id_документа_окончания_связи).*

Шаг 14. Если в результате выполнения транзакции значения атрибутов массива записей *array_rel* не меняются, то перейти к Шагу 16.

Шаг 15. Принять значение переменной *stage_number=4* и перейти к Шагу 19.

Шаг 16. Сформировать массив записей *array_ident*, для которых справедливо условие (*Описание_НД.Id_документа = Описание_тождественности_НД.Id_базового_документа).*

Шаг 17. Если в результате выполнения транзакции значения атрибутов массива записей *array_ident* не меняются, то перейти к Шагу 19.

Шаг 18. Принять значение переменной *stage_number=5* и перейти к Шагу 19.

Шаг 19. Передать значение переменной *stage_number* в обобщенный алгоритм выполнения функции решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия, состоит из следующих шагов.

Диаграмма деятельности алгоритма применения метода решения подзадачи определения достоверности состава, содержания и взаимодействия

НД d_i с другими НД из БНД предприятия за период актуальности данного НД в рамках БНД предприятия приведена на рисунке 3.9.

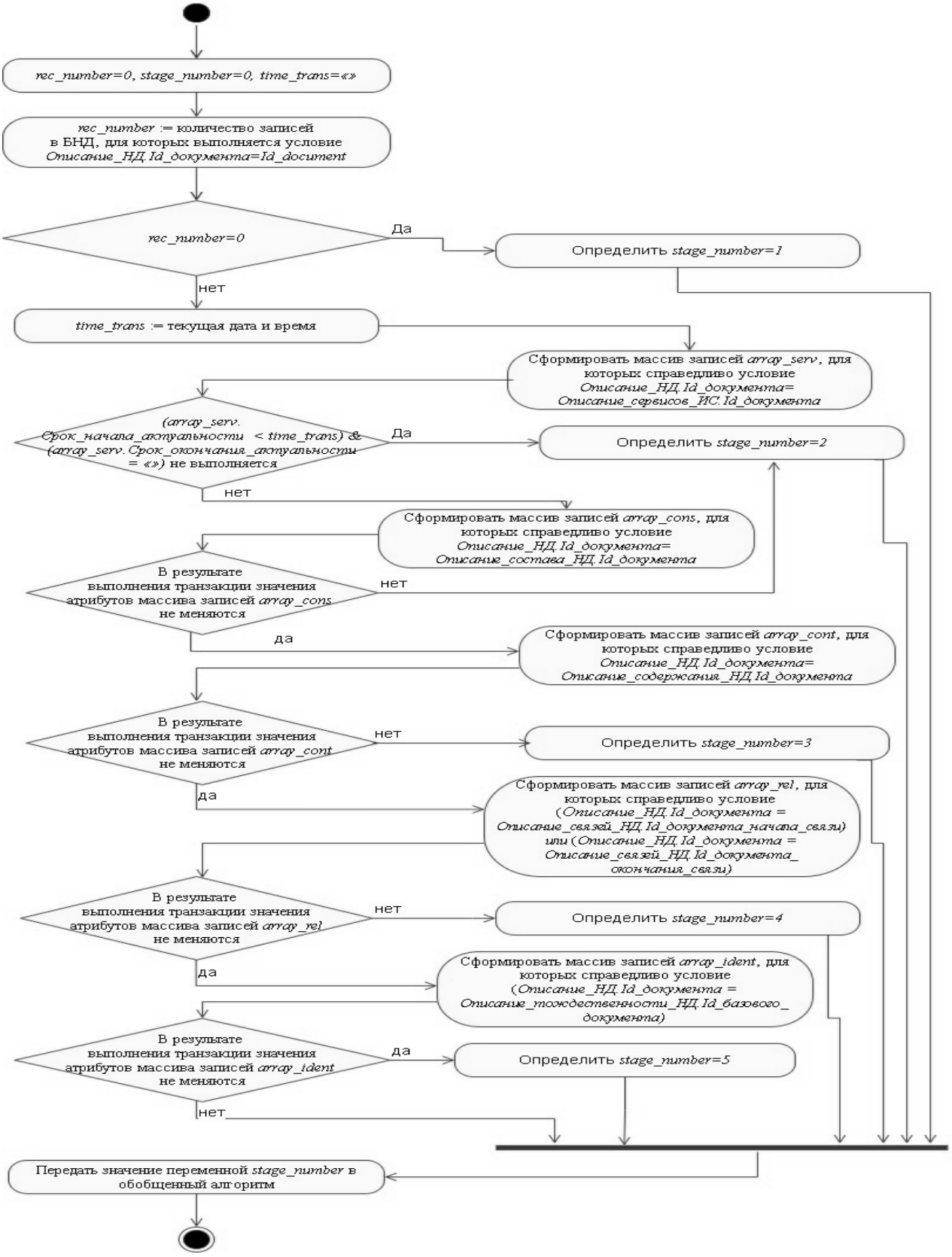

Рисунок 3.9 – Диаграмма деятельности алгоритма применения метода решения подзадачи определения достоверности

Соответствие шагов алгоритма применения метода решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД в рамках БНД предприятия и этапов данного метода рассмотрено в таблице 3.2.

Для удобства определения предикаты Этапов 2, 3 и 4 метода решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД в рамках БНД предприятия разделены в алгоритме на ряд меньших предикатов. При этом вначале проверяется достоверность сервиса, через который пытаются изменить состав, содержание, взаимодействие или тождественность описаний НД d_i (Шаги 5 и 6), поскольку данная проверка является составной частью всех упомянутых выше предикатов.

Таблица 3.2 – Соответствие шагов алгоритма применения метода решения подзадачи определения достоверности состава, содержания и взаимодействия нормативного документа d_i с другими нормативными документами из базы нормативных документов предприятия за период актуальности данного нормативного документа в рамках базы нормативных документов предприятия и этапов данного метода

Шаги алгоритма	Этапы метода
Шаг 1 – Шаг 3	Этап 1
Шаг 4 – Шаг 9	Этап 2
Шаг 10 – Шаг 12	Этап 3
Шаг 13 – Шаг 15	Этап 4
Шаг 16 – Шаг 19	Этап 5

Далее проверяется достоверность описаний состава НД d_i (Шаги 7, 8 и 9). После этого проверяется достоверность возможного содержания НД d_i (Шаги 10, 11 и 12). После этого проверяется достоверность возможного взаимодействия НД d_i с другими НД (Шаги 13, 14 и 15). После этого проверяется достоверность тождественности НД d_i другим НД (Шаги 16, 17 и 18).

Конкретный вид предложенных в данном подразделе алгоритмов может меняться измениться с учетом особенностей платформ, применяемых разработчиками конкретной реализации информационной технологии.

3.4 Разработка алгоритмов решения подзадачи определения неизменности базы нормативных документов

Как показано на рисунке 3.4, в основе алгоритма выполнения функции решения подзадачи определения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия лежит алгоритм применения метода решения подзадачи определения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия, рассмотренный в подразделе 2.2. Поэтому предлагается рассматривать алгоритм выполнения функции

решения подзадачи определения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия как совокупность двух следующих частей:

а) обобщенный алгоритм выполнения функции, назначение которого аналогично рассмотренным в подразделе 3.2 и подразделе 3.3 назначениям обобщенных алгоритмов выполнения функций решения соответствующих подзадач;

б) алгоритм применения метода решения подзадачи определения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия.

Обобщенный алгоритм выполнения функции решения подзадачи определения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия состоит из следующих шагов.

Шаг 1. Переменной *result_function_determine_immutability* присвоить значение 0, переменной *name_result_fdi* присвоить значение «Проверка неизменности начата».

Шаг 2. Получить значения переменных *result_function_determine_authenticity* и *Id_document,* определенные по результатам выполнения функции решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия.

Шаг 3. Если *result_function_determine_ authenticity =0,* то переменной *name_result_fdi* присвоит значение «Проверка незименности не проводилась» и перейти на Шаг 7.

Шаг 4. Выполнить алгоритм применения метода решения подзадачи определения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия.

Шаг 5. Если алгоритм, выполненный на Шаге 4, завершен успешно, то присвоить переменной *result_function_determine_immutability* значение 1, а переменной *name_result_fdi* присвоить значение «Проверка достоверности выполнена успешно». После этого перейти к Шагу 7.

Шаг 6. Если получено сообщение о попытке несанкционированного изменения БНД, то присвоить переменной *result_function_determine_immutability* значение 0, а переменной *name_result_fdi* в зависимости от того, на каком этапе метода была обнаружена ошибка, присвоить одно из следующих значений:

а) значение «Попытка несанкционированного изменения НД с идентификатором *Id_document*» (ошибка обнаружена в ходе выполнения Этапа 1 метода);

б) значение «Попытка нарушения неизменности описания состава НД d_i в БНД предприятия» (ошибка обнаружена в ходе выполнения Этапа 2 метода);

в) значение «Попытка нарушения неизменности описания возможного содержания НД d_i в БНД предприятия» (ошибка обнаружена в ходе выполнения Этапа 3 метода);

г) значение «Попытка нарушения неизменности описаний взаимодействия НД d_i с конкретными НД d_k в БНД предприятия» (ошибка обнаружена в ходе выполнения Этапа 4 метода);

д) значение «Попытка нарушения неизменности тождественности описаний НД d_i и описаний конкретных НД d_k в БНД предприятия» (ошибка обнаружена в ходе выполнения Этапа 5 метода).

Шаг 7. Передать значения переменных *result_function_determine_immutability*, *Id_document* и *name_result_fdi* в другие функции информационной технологии и завершить выполнение алгоритма.

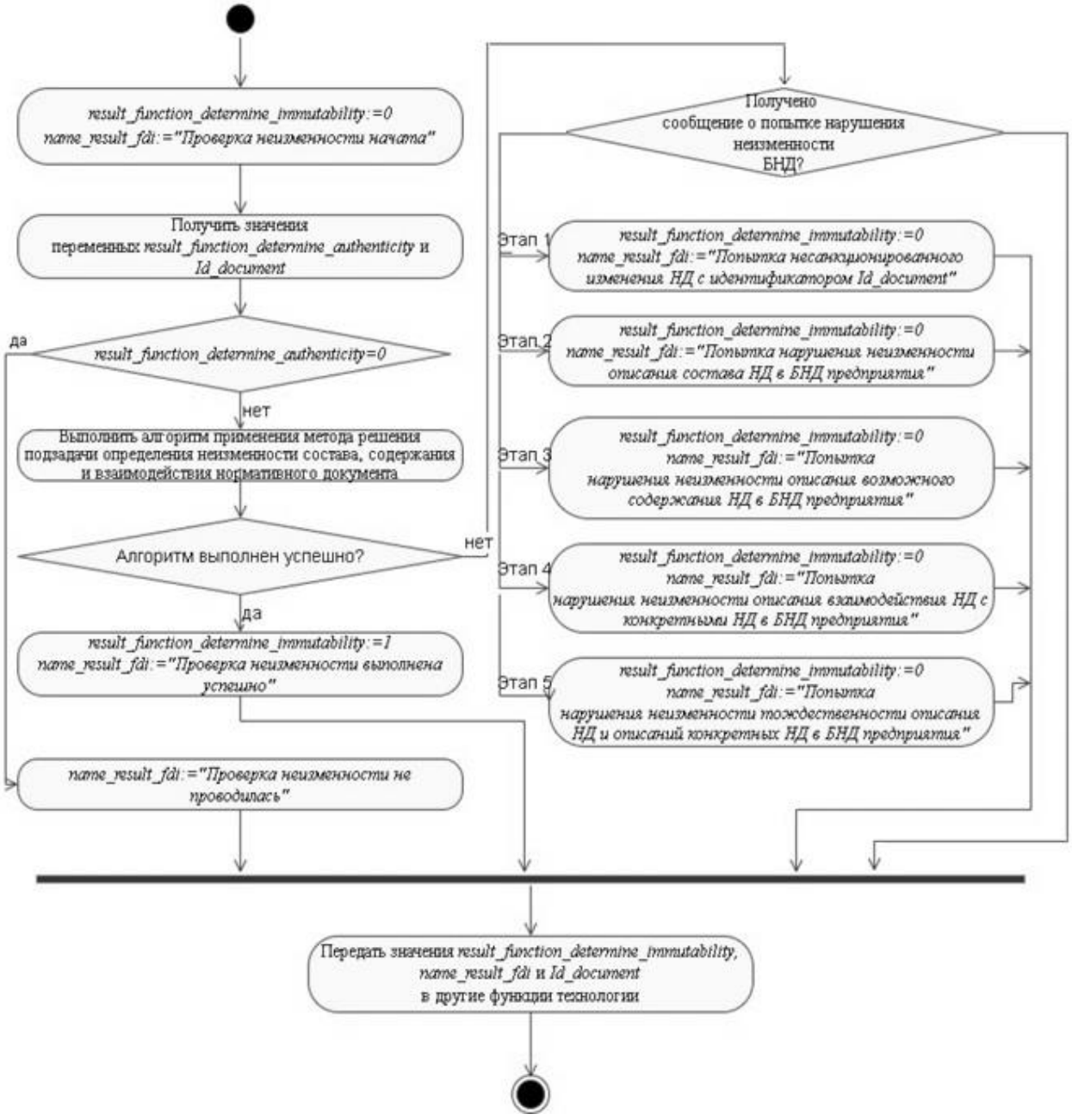

Рисунок 3.10 – Диаграмма деятельности обобщенного алгоритма выполнения функции решения подзадачи определения неизменности состава, содержания и взаимодействия нормативного документа d_i в рамках базы нормативных документов предприятия

В соответствии с рисунком 3.10 приведена, диаграмма деятельности обобщенного алгоритма выполнения функции решения подзадачи определения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия.

Алгоритм применения метода решения подзадачи обеспечения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия состоит из следующих шагов.

Шаг 1. Определить значения переменных *rec_number=0, stage_number=0, time_trans=«».*

Шаг 2. Установить значение переменной *rec_number* как количество записей в БНД, для которых выполняется условие *Описание_НД.Id_документа=Id_document*.

Шаг 3. Если *rec_number=0*, то переменной *stage_number* присвоить значение 1 и перейти к Шагу 18.

Шаг 4. Установить значение переменной *time_trans* как текущую дату и время.

Шаг 5. Сформировать массив записей *array_cons*, для которых справедливо условие *(Описание_НД.Id_документа=Описание_состава_НД.Id_документа) & (Описание_НД. Срок_начала_актуальности <time_trans) & (Описание_НД. Срок_окончания_актуальности = «»)*.

Шаг 6. Если в результате выполнения транзакции значения атрибутов массива записей *array_cons* не меняются, то перейти к Шагу 8.

Шаг 7. Принять значение переменной *stage_number=2* и перейти к Шагу 18.

Шаг 8. Сформировать массив записей *array_cont*, для которых справедливо условие *(Описание_НД.Id_документа=Описание_содержания_НД.Id_документа) & (Описание_НД. Срок_начала_актуальности < time_trans) & (Описание_НД. Срок_окончания_актуальности = «»)*.

Шаг 9. Если в результате выполнения транзакции значения атрибутов массива записей *array_cont* не меняются, то перейти к Шагу 11.

Шаг 10. Принять значение переменной *stage_number=3* и перейти к Шагу 18.

Шаг 11. Сформировать массив записей *array_rel*, для которых справедливо условие *((Описание_НД.Id_документа = Описание_связей_НД.Id_документа_начала_связи) или (Описание_НД.Id_документа = Описание_связей_НД.Id_документа_окончания_связи)) & (Описание_НД. Срок_начала_актуальности < time_trans) & (Описание_НД. Срок_окончания_актуальности = «»)*.

Шаг 12. Если в результате выполнения транзакции значения атрибутов массива записей *array_rel* не меняются, то перейти к Шагу 14.

Шаг 13. Принять значение переменной *stage_number=4* и перейти к Шагу 18.

Шаг 14. Сформировать массив записей *array_ident*, для которых справедливо условие (*Описание_НД.Id_документа = Описание_тождественности_НД.Id_базового_документа) & (Описание_НД. Срок_начала_актуальности < time_trans) & (Описание_НД. Срок_окончания_актуальности = «»)*.

Шаг 15. Если количество записей в массиве равно 0, то перейти к Шагу 18.

Шаг 16. Если в результате выполнения транзакции значения атрибутов массива записей *array_ident* не меняются, то перейти к Шагу 17.

Шаг 17. Принять значение переменной *stage_number=5* и перейти к Шагу 18.

Шаг 18. Передать значение переменной *stage_number* в обобщенный алгоритм выполнения функции решения подзадачи обеспечения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия.

Диаграмма деятельности алгоритма применения метода решения подзадачи обеспечения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия приведена на рисунке 3.11.

Соответствие шагов алгоритма применения метода решения подзадачи обеспечения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия и этапов данного метода рассмотрено в таблице 3.3.

Таблица 3.3 – Соответствие шагов алгоритма применения метода решения подзадачи определения неизменности состава, содержания и взаимодействия нормативного документа d_i в рамках базы нормативных документов предприятия и этапов данного метода

Шаги алгоритма	Этапы метода
Шаг 1 – Шаг 3	Этап 1
Шаг 4 – Шаг 7	Этап 2
Шаг 8 – Шаг 10	Этап 3
Шаг 11 – Шаг 13	Этап 4
Шаг 14 – Шаг 18	Этап 5

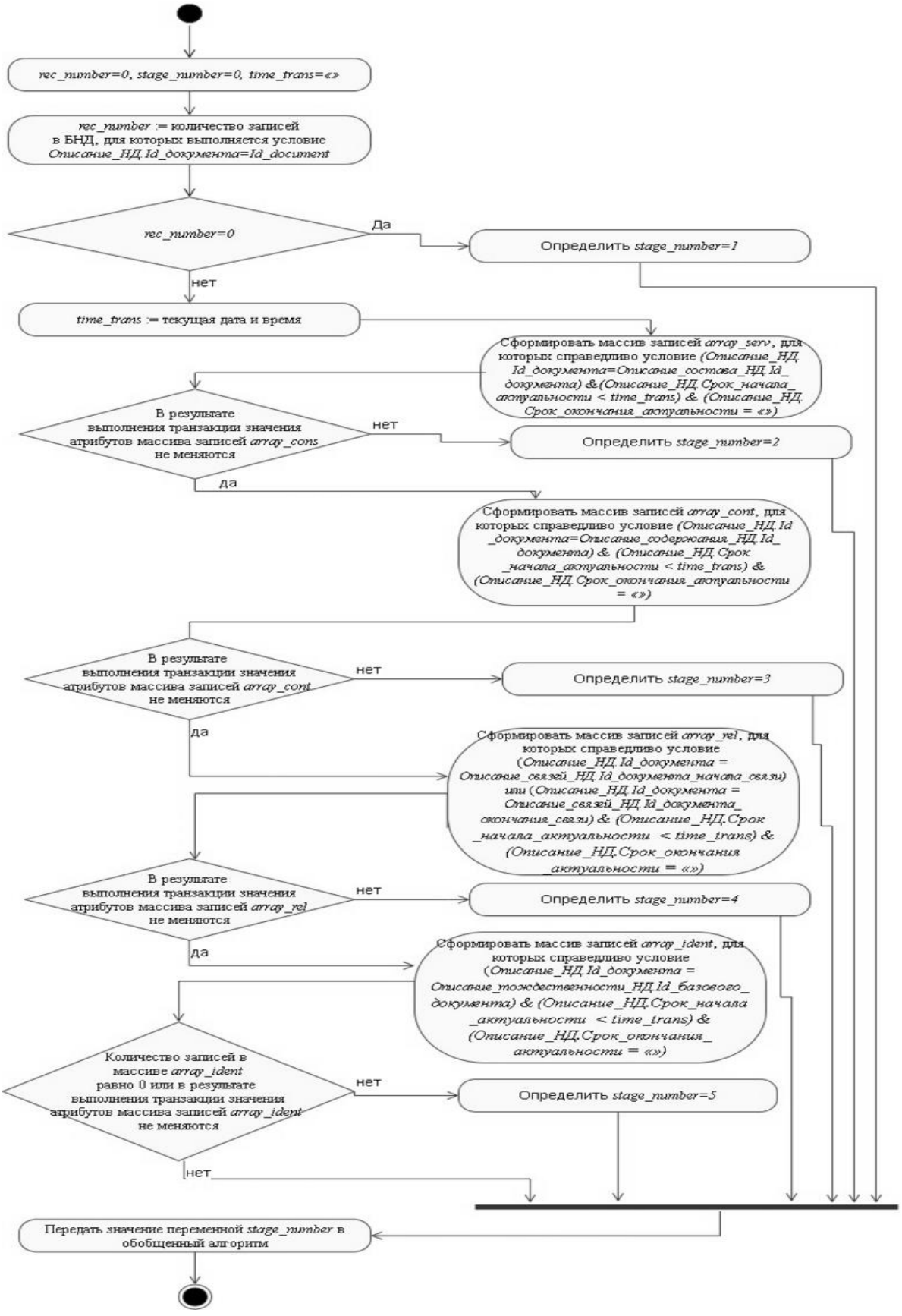

Рисунок 3.11 – Диаграмма деятельности алгоритма применения метода решения подзадачи определения неизменности

Выводы к третьему разделу

1. Для достижения поставленной цели исследования разработана информационная технология обеспечения целостности базы нормативных документов предприятия. В ходе разработки информационной технологии были определены особенности взаимодействия этой информационной технологии с другими элементами СУП. Разработана диаграмма потоков данных, которая описывает основные функции предлагаемой информационной технологии. Разработана диаграмма «сущность – связь», которая описывает концептуальную модель данных предлагаемой информационной технологии. С использованием диаграммы SwimLane описана последовательность работ, выполняемых в рамках каждой функции предлагаемой информационной технологии.

2. Разработан алгоритм решения подзадачи определения субъектов, имеющих право на изменение базы нормативных документов предприятия. Предложено разделить данный алгоритм на две основные части: обобщенный алгоритм выполнения соответствующей функции и алгоритм применения метода решения подзадачи определения субъектов ИС, имеющих права на изменение состава, содержания и взаимодействия НД d_i в рамках БНД предприятия. Алгоритмы представлены в текстовом виде и в виде диаграмм деятельностей UML.

3. Разработан алгоритм решения подзадачи определения достоверности базы нормативных документов. Предложено разделить данный алгоритм на две основные части: обобщенный алгоритм выполнения соответствующей функции и алгоритм применения метода решения подзадачи определения достоверности состава, содержания и взаимодействия НД d_i с другими НД из БНД предприятия за период актуальности данного НД в рамках БНД предприятия. Алгоритмы представлены в текстовом виде и в виде диаграмм деятельностей UML.

4. Разработан алгоритм решения подзадачи определения неизменности базы нормативных документов. Предложено разделить данный алгоритм на две основные части: обобщенный алгоритм выполнения соответствующей функции и алгоритм применения метода решения подзадачи обеспечения неизменности состава, содержания и взаимодействия НД d_i в рамках БНД предприятия. Алгоритмы представлены в текстовом виде и в виде диаграмм деятельностей UML.

ЗАКЛЮЧЕНИЕ

В современных системах происходит переориентация на процессное управление, что приводит к регулярным изменениям регламентирующей базы нормативных документов, правильное и своевременное обновление которой, а также сохранение ее гарантоспособности, становится одной из важных задач, стоящих перед системой, участвующей в управлении бизнес-процессами.

Внедрение системы контроля целостности базы нормативных документов позволяет системам эффективно управлять регламентирующими компонентами подсистем управления бизнес-процессами, обеспечивая их актуальность, достоверность и своевременность, соответствие объектов управления действующим версиям субъектов управления - нормативных документов вышестоящих уровней иерархии.

Для обеспечения гарантоспособности и систематизации базы нормативных документов посредством придания ей свойства целостности поставлена цель исследования - разработка моделей и методов контроля целостности и управления процессами внесения изменений в базу нормативных документов.

Для реализации формализованного подхода к решению задачи контроля целостности базы нормативных документов использованы методологические подходы, заключающиеся в применении:

– алгебры предикатов для постановки задачи и формирования агрегированной модели обеспечения контроля целостности базы нормативных документов;

– декларативных фреймовых моделей и методов обеспечения контроля целостности для описания нормативной базы и аппарата целостности с позиций системности и целостности описания;

– семантических моделей для формализации представления базы нормативных документов и их взаимосвязей.

В ходе исследования поставлены и решены следующие задачи, позволившие придать согласованность базе нормативных документов и уменьшить вариативность в параметрах управления бизнес-процессами:

– разработаны модели обеспечения контроля целостности базы нормативных документов;

– разработаны методы обеспечения неизменности, определения субъектов информационной системы и достоверности состава, содержания и взаимодействия нормативных документов;

– разработаны достаточные условия для выполнимости требований методов обеспечения неизменности, определения субъектов информационной системы и достоверности состава, содержания и взаимодействия нормативных документов;

– разработаны алгоритмы реализации методов обеспечения неизменности, определения субъектов информационной системы и

достоверности состава, содержания и взаимодействия нормативных документов;

– разработаны модели информационно-аналитической системы контроля целостности базы нормативных документов как результат взаимно-однозначного (биективного) отображения фреймовых моделей представления базы нормативных документов в элементы проектируемой системы.

Таким образом, результаты исследования позволяют повысить эффективность использования и управления параметрами и показателями сопровождения и управления бизнес-процессами за счет:

– устранения противоречивости значений параметров управления процессами, установленных разными документами;

– формирования стратегии поддержания целостности базы нормативных документов;

– однозначности регламентации процессного подхода к управлению базой нормативных документов и бизнес-процессами;

– формирования обратной связи между объектами и субъектами базы нормативных документов в управлении бизнес-процессами.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Баскакова О.В., Л.Ф. Экономика предприятия (организации): учеб. – М.: Дашков и К, 2013. – 372 с.

2 Кухаренко Е.В., Оспанова Г.Ж. К вопросу оценки качества нормативной базы // Вестник Алматинского университета энергетики и связи. – 2020. – №1. – С. 62-67.

3 ГОСТ 1.1-2002. Термины и определения. – Введ. 2003-07-01. – М.: ИПК Издательство стандартов, 2003. – 40 с.

4 ГОСТ Р 1.12-2020. Термины и определения. – Введ. 2020-09-01. – М.: Стандартинформ, 2020. – 10 с.

5 ГОСТ Р 1.4-2004. Стандарты организаций. Общие положения. – Введ. 2005-07-01. – М.: Стандартинформ, 2018. – 8 с.

6 Цапко Е.А. Стандартизация: учеб.-метод. пос. – Томск, 2010. – 92 с.

7 Крылова Г.Д. Основы стандартизации, сертификации, метрологии. – Изд. 3-е, перер. и доп. – М.: ЮНИТИ-ДАНА, 2003. – 671 с.

8 Марусина М.Я., Ткалич В.Л., Воронцов Е.А. и др. Основы метрологии, стандартизации и сертификации. – СПб.: СПбГУ ИТМО, 2009. – 164 с.

9. Кравченко Е.В., Кривогузова Ю.К., Озерова И.П. Метрология, стандартизация и сертификация. − Томск, 2013. – 172 с.

10 Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. – СПб.: Питер, 2017. – 256 с.

11 Лифиц И.М. Стандартизация, метрология и сертификация. – Изд. 5-е, перер. и доп. – М.: Юрайт-Издат. 2005. – 345 с.

12 Варзунов А.В., Торосян Е.К., Сажнева Л.П. Анализ и управление бизнес-процессами. – СПб.: Университет ИТМО, 2016. – 112 с.

13 Репин В.В. Бизнес-процессы. Моделирование, внедрение, управление. – М.: Манн, Иванов и Фербер, 2013. – 512 с.

14 Бобылева М.П. Управленческий документооборот: от бумажного к электронному. – М., 2010. – 410 с.

15 Нечаева Е.В. Делопроизводство. – СПб., 2015. – 178 с.

16 Куриленко А.Н., Кокиц Е.В. Делопроизводство: курс лекций. – Горки: БГСХА, 2019. – 70 с.

17 Демин Ю.М. Делопроизводство. Подготовка служебных документов. – Изд. 3-е, перер. и доп. – СПб.: Питер, 2009. – 256 с.

18 Басаков М.И. Делопроизводство и корреспонденция в вопросах и ответах. – Изд. 5-е, перер. и доп. – Р-на-Д.: Феникс, 2003. – 320 с.

19 Мифтахова Н.И. Метрология, стандартизация и сертификация. – Нижнекамск, 2018. – 100 с.

20 Шишмарёв В.Ю. Метрология, стандартизация, сертификация и техническое регулирование. – Изд. 6-е, испр. – М.: Академия, 2016. – 320 с.

21 Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. – Введ. 2006-06-01. – М.: Стандартинформ, 2006. – 20 с.

22 Радченко М.Г., Хрусталева Е.Ю. Архитектура и работа с данными «1С:Предприятия 8.2». – М., 2011. – 268 с.

23 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2008-02-01. – М.: Стандартинформ, 2008. – 12 с.

24 ГОСТ 33707-2016 (ISO/IEC 2382:2015). Информационные технологии. Словарь. – Введ. 2017-09-01. – М.: Стандартинформ, 2016. – 206 с.

25 ГОСТ ISO 9000-2011. Системы менеджмента качества. Основные положения и словарь. – Введ. 2013-01-01. – М.: Стандартинформ, 2018. – 32 с.

26 Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. – Введ. 2006-01-01. – М.: Стандартинформ, 2005. – 16 с.

27 ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – Введ. 2007-08-01. – М.: Стандартинформ, 2007. – 23 с.

28 Ясенев В.Н., Дорожкин А.В., Сочков А.Л. и др. Информационная безопасность. – Нижний Новгород, 2017. – 198 с.

29 Ясенев В.Н. Конспект лекций по информационной безопасности. – Нижний Новгород, 2017. – 254 с.

30 Ярочкин В.И. Информационная безопасность. – Изд. 2-е. – М., 2004. – 544 с.

31 Оспанова Г.Ж., Кухаренко Е.В. Мировой опыт системы контроля и управления целостности нормативной базы // Вестник КазНИТУ им. К. Сатпаева. – 2020. – №1. – С. 350-354.

32 Громов Ю.Ю., Дидрих И.В., Иванова О.Г. и др. Информационные технологии. – Тамбов, 2015. – 260 с.

33 Вострецова Е.В. Основы информационной безопасности. – Екатеринбург: Изд-во Урал. Ун-та, 2019. – 204 с.

34 Скакун В.В. Защита информации в базах данных и экспертных системах. – Минск, 2015. – 140 с.

35 Кухаренко Е.В., Оспанова Г.Ж. Модели обеспечения целостности нормативной базы // Вестник КазНИТУ. – 2019. – №6. – С. 347-351.

36 Макаренко С.И. Информационная безопасность: учеб. пос. – Ставрополь, 2009. – 372 с.

37 Кэмпбелл Л., Мейджорс Ч. Базы данных. Инжиниринг надежности. – СПб.: Питер, 2020. – 304 с.

38 Карпова И.П. Базы данных. – М., 2009. – 131 с.

39 Введение в криптографию / под ред. В.В. Ященко. – Изд. 4-е, доп. – М.: МЦНМО, 2012. – 348 с.

40 Голиков А.М. Основы информационной безопасности. – Томск, 2007. – 288 с.

41 ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. – Введ. 1996-01-01. – М.: Издательство стандартов, 1995. – 8 с.

42 Смарт Н. Криптография / пер. с англ. – М.: Техносфера, 2005. – 528 с.

43 Гатченко Н.А., Исаев А.С., Яковлев А.Д. Криптографическая защита информации. – СПб., 2012. – 142 с.

44 ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – Введ. 2019-06-01. – М.: Стандартинформ, 2018. – 20 с.

45 ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хэширования. – Введ. 2019-06-01. – М.: Стандартинформ, 2018. – 23 с.

46 Гайдамакин Н.А. Теоретические основы компьютерной безопасности: учеб. пос. – Екатеринбург: Изд-во Урал. Ун-та, 2008. – 212 с.

47 Голицына О.Л., Максимов Н.В., Попов И.И. Базы данных. – Изд. 2-е, испр. и доп. – М., 2009. – 400 с.

48 Мамедли Р.Э. Системы управления базами данных: учеб. пос. – Нижневартовск, 2021. – 214 с.

49 Новиков Б.А., Горшкова Е.А., Графеева Н.Г. Основы технологий баз данных: учеб. пос. – Изд. 2-е. – М.: ДМК Пресс, 2020. – 582 с.

50 Кузнецов С.Д. Основы баз данных. – Изд. 2-е, испр. – М., 2007. – 484 с.

51 Куликов С.С. Реляционные базы данных в примерах: практическое пособие для программистов и тестировщиков. – Минск, 2020. – 424 с.

52 Марков А.С., Лисовский К.Ю. Базы данных. Введение в теорию и методологию. – М.: Финансы и статистика, 2006. – 512 с.

53 Дейт К.Дж. Введение в системы баз данных / пер. с англ. – М.: Вильямс, 2006. – 1328 с.

54 Пушкарев А.В., Новиков С.Н. Анализ подходов обеспечения целостности информации // Интерэкспо Гео-Сибирь. – 2019. – Т. 6, №1. – С. 122-127.

55 Диченко С.А. Контроль и обеспечение целостности информации в системах хранения данных. // Наукоемкие технологии в космических исследованиях Земли. – 2019. – Т. 11, №1. – С. 49-57.

56 Диченко С.А., Финько О.А. Обобщенный способ применения хэш-функции для контроля целостности данных // Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12, №6. – С. 48-59.

57 Киселев Д.В., Семенов С.С., Петров О.В. Методика обеспечения целостности информации в программно-аппаратных комплексах связи за счет рационального резервирования // Системы управления, связи и безопасности. – 2019. – №1. – С. 204-220.

58 Oh S., Cho S., Han S. et al. Pre-verification of Data in Electronic Trade Blockchain Platform // In book: Data Science and Digital Transformation in the Fourth Industrial Revolution. – Cham: Springer, 2021. – P. 53-65.

59 Adnan Md.N. et al. An Innovative Approach of Verification Mechanism for both Electronic and Printed Documents // International Journal of Advanced Computer Science and Applications. – 2020. – Vol. 11, Issue 8. – P. 623-627.

60 Бородин А.В., Никитин Р.Ю., Ширяев А.И. Обеспечение целостности и подлинности критической информации на бумажном носителе при отчужденной обработке документа // Приоритетные направления развития науки и образования. – 2016. – №3. – С. 83-87.

61 Еременко А.В., Сулавко А.Е., Толкачева Е.В. и др. Метод защиты текстовых документов на электронных и бумажных носителях на основе скрытого биометрического идентификатора субъекта, получаемого из подписи. // Информационные технологии. – 2016. – Т. 22, №8. – С. 628-634.

62 Сагайдак Д.А., Файзуллин Р.Т. Способ формирования цифрового водяного знака для физических и электронных документов // Компьютерная оптика. – 2014. – Т. 38, №1. – С. 94-104.

63 Бобылева М.П. К вопросу о целостности и аутентичности управленческих электронных документов в процессе их хранения // Делопроизводство. – 2018. – №3. – С. 33-39.

64 Лапина Т.И., Димов Э.М., Петрик Е.А. и др. Управление доступом к информационным ресурсам в информационных системах // Моделирование, оптимизация и информационные технологии. – 2018. – Т. 6, №4. – С. 523-534.

65 Лачихина А.Б., Костикова Е.Е. Вопросы обеспечения целостности в базах данных корпоративных информационных систем на базе СУБД SQL Server // Вопросы радиоэлектроники. – 2016. – №10. – С. 9-12.

66 Saxena R., Dey S. Cloud audit: A data integrity verification approach for cloud computing // Procedia Computer Science. – 2016. – Vol. 89. – P. 142-151.

67 Rohde T., Chupalov R., Shulman N. et al. Audit logs to enforce document integrity in Skyline and Panorama // Bioinformatics. – 2020. – Vol. 36, Issue 15. – P. 4366-4368.

68 Brunner C., Knirsch F., Engel D. SPROOF: A Platform for Issuing and Verifying Documents in a Public Blockchain // Proceed. of the 5th internat. conf. on Information Systems Security and Privacy. – Prague, 2019. – P. 15-25.

69 Páez R., Pérez M., Ramírez G. et al. An Architecture for Biometric Electronic Identification Document System Based on Blockchain // Future Internet/ - 2020. – Vol. 12, Issue 11. – P. 10-1-10-19.

70 Fernando A.B. et al. The Design of Smart Cashless Transaction // Procced. 5th internat. conf. on Intelligent Information Technology (ICIIT 2020). – NY., 2020. – P. 86-90.

71 Буренков В.С., Кулагин Д.А. Модель мандатного контроля целостности в операционной системе KasperskyOS // Тр. ИСП РАН. – 2020. – Т. 32, вып. 1. – С. 27-56.

72 Yang X., Li T., Xi W. et al. A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRS sharing in the cloud // IEEE Access. – 2020. – Vol. 8. – P. 170713-170731.

73 Nirjhor M.K.I., Yousuf M.A., Mhaboob M.S. Electronic Medical Record Data Sharing through Authentication and Integrity Management // Procced. 2nd internat. conf. on Robotics, Electrical and Signal Processing (ICREST 2021). – Dhaka, 2021. – P. 308-313.

74 Гартвич А.В. Планирование закупок, производства и продаж в 1С: Предприятии 8. – СПб.: Питер, 2007. – 160 с.

75 Бойко Э.В. 1С: Предприятие 8.0. Универсальный самоучитель. – М.: Омега-Л, 2010. – 232 с.

76 Филатова В.О. 1С: Предприятие 8.3. Бухгалтерия предприятия, управление торговлей, управление персоналом. – СПб.: Питер, 2014. – 240 с.

77 Утилита контроля целостности // https://v8.1c.ru/platforma/utilita-kontrolya-celostnosti. 28.08.2021.

78 Елашкин М. SAP Business One. Строим эффективный бизнес. – М., 2007. – 240 с.

79 Хагеман С., Вилл Л. SAP R/3. Системное администрирование. – М.: Лори, 2007. – 480 с.

80 Кале В. Внедрение SAP R/3: руков. для менеджеров и инженеров / пер. с англ. – М.: Компания АйТи, 2006. – 511 с.

81 Ненашев С.А. Криптографическая защита информации в ERP-системах компании SAP // Информационная безопасность. – 2009. – №3. – С. 24-25.

82 Кугушева Т.В., Болгов В.Е. Перспективы развития системы электронного документооборота "ДЕЛО" на российском рынке автоматизированных информационных систем // Журнал «У» Экономика. Управление. Финансы. – 2020. – №2. – С.151-162.

83 Ушаков Н.О., Сибикина И.В., Космачева И.М. Информационная безопасность в системах электронного документооборота. // Техническая эксплуатация водного транспорта: проблемы и пути развития. – 2021. – №1. – С. 70-74.

84 Приходько Ю.С., Долгова Т.Г. «Дело» – система электронного документооборота в России // Актуальные проблемы авиации и космонавтики. – 2011. – №7. – С. 458-459.

85 Власова Л.А. Проблема выбора СЭД для предприятий. // Вестник Хабаровского государственного университета экономики и права. – 2020. – №1-2 (102-103). – С. 88-98.

86 Приложение ELMA ECM+: краткое руководство // https://www.elma-bpm.ru/KB/help/elma_ecm_quick_start.pdf. 29.08.2021.

87 Чебескова С.А., Яковлева А.О. Совершенствование системы электронного документооборота на примере СК Согласие // Актуальные исследования. – 2019. – №3 – С. 81-85.

88 Семенова А.А., Глухов Н.И. Некоторые аспекты анализа системы защиты электронного документооборота// Информационные технологии и математическое моделирование в управлении сложными системами – 2019. – №3. – С. 42-46.

89 Веселков А.Н., Кузнецов В.Н., Доропей В.Н. Информационная система поддержки нечеткой оценки и согласованной оптимизации // Программные продукты и системы. – 2015. – №2(110). – С. 140-144.

90 Игнатова И.Г. и др. Система автоматизации документооборота университета с учетом специфики сферы деятельности // Известия высших учебных заведений. Электроника. – 2014. – №3(107). – С. 81-91.

91 Поддубный М.И. Новый подход к построению моделей безопасности систем электронного документооборота// Инженерный вестник Дона. – 2023. – №2(98). – С. 235-245.

92 Кубеков Б.С. Моделирование информационных систем на базе модели Захмана и онтологическом инжиниринге // Интеллектуальные технологии на транспорте. – 2023. – №1(35-1). – С. 129-133.

93 Минский М. Фреймы для представления знаний. – М.: Энергия, 1979. – 152 с.

94 Lassila O. Frames or Objects, or Both? // Workshop Notes from the Eight nat. conf. on Artificial Intelligence (AAAI-90). – Boston, 1990. – P. 1-8.

95 Wu X. A Comparison of Objects with Frames and OODBs // Object Currents. – 1996. – Vol. 1, Issue 1. – P. 1-9.

96 Гаврилов, А.В. Системы искусственного интеллекта. – Новосибирск: НГТУ, 2004. – 59 с.

97 Левыкин В.М. и др. Исследование и разработка фреймовой модели структуры документа // Новые технологии. – 2008. – №1(19). – С. 149-154.

98 Ospanova G., Kukharenko E., Ievlanov M. et al. Building a model of the integrity of information resources within an enterprise management system // Eastern-European Journal of Enterprise Technologies. – 2021. – Vol. 3, Issue 2(111). – P. 15-23.

99 Воронцов Ю.А., Козинец А.В. Стандарты веб-сервисов для создания распределенных информационных систем // Век качества. – 2015. – №3. – С. 55-72.

100 Билалова Д.Г.-К., Магомедов Н.Н. Понятие электронной цифровой подписи // Инновационная наука. – 2022. – №2-1. – С. 6-8.

101 Деревянко А.С., Солощук М.Н. Технологии и средства консолидации информации: учеб. пос. – Харьков, 2008. – 432 с.

102 Дворяк Д.А. Сравнение технологий REST И SOAP на основе возможностей создания web-сервисов // Вестник науки. – 2024. – №1(70). – С. 448-465.

103 Дергачев А.М., Кореньков Ю.Д., Логинов И.П. и др. Технологии веб-сервисов. – СПб., 2021. – 100 с.

104 Машнин Т.С. Web-сервисы Java. – СПб.: БХВ-Петербург, 2012. – 560 с.

105 Белалова Г.А. Анализ методов интеграции информационных систем // Цифровые модели и решения. – 2023. – №3. – С. 61-68.

106 Оспанова Г.Ж. Информационно аналитическая система управления нормативной базой // Матер. междунар. науч.-практ. конф. «Глобальная наука и инновации: Центральная Азия». – Нур-Султан, 2019. – С. 321-327.

107 Кухаренко Е.В., Оспанова Г.Ж. Нормативті базаны үйымдастуруда тұтастық теориясын қолдану // Матер. междунар. науч.-практ. конф. «Стандартизация инструмент повышения конкурентоспособности и интеграции

казахстанской продукции, в мировую экономику». – Нур-Султан, 2019. – С. 120-125.

108 Никифорова А.А. Методология RUP как эффективное средство разработки программного обеспечения// E-Scio. – 2023. – №3(78). – С. 86-93.

109 Десятков П.А., Кряжева Е.В. Проектирование модуля-конвертера для 1С: Предприятие // Научные известия. – 2022. – №29. – С. 50-54.

ПРИЛОЖЕНИЕ А

Свидетельство об авторском праве

КАЗАҚСТАН РЕСПУБЛИКАСЫ

РЕСПУБЛИКА КАЗАХСТАН

СВИДЕТЕЛЬСТВО

О ВНЕСЕНИИ СВЕДЕНИЙ В ГОСУДАРСТВЕННЫЙ РЕЕСТР ПРАВ НА ОБЪЕКТЫ, ОХРАНЯЕМЫЕ АВТОРСКИМ ПРАВОМ

№ 44395 от «12» апреля 2024 года

Фамилия, имя, отчество, (если оно указано в документе, удостоверяющем личность) автора (ов):
ОСПАНОВА ГУЛЬМИРА ЖАБАЕВНА; Кухаренко Евгения Владимировна

Вид объекта авторского права: **произведение науки**

Название объекта: **Модель обеспечения целостности базы нормативных документов**

Дата создания объекта: **09.04.2024**

Подписано ЭЦП

Е. Осланов