ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 70924— 2023 (ИСО/МЭК 30141: 2018)

Информационные технологии

ИНТЕРНЕТ ВЕЩЕЙ

Типовая архитектура

[ISO/IEC 30141:2018, Internet of Things (IoT) — Reference Architecture, MOD]

Издание официальное

Москва
Российский институт стандартизации
2023

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным образовательным учреждением высшего образования «МИРЭА — Российский технологический университет» (РТУ МИРЭА) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 194 «Кибер-физические системы»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 ноября 2023 г. № 1474-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 30141:2018 «Интернет вещей (ИВ). Типовая архитектура» [ISO/IEC 30141:2018 «Internet of Things (IoT) — Reference Architecture», MOD] путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом. Внесение указанных технических отклонений направлено на учет потребностей национальной экономики Российской Федерации.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

5 ВВЕДЕН ВПЕРВЫЕ

6 ДЕЙСТВУЕТ ВЗАМЕН ПНСТ 438—2020

7 Некоторые элементы настоящего стандарта могут быть объектами патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за установление подлинности каких-либо или всех таких патентных прав

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© ISO, 2018
© IEC, 2018
© Оформление. ФГБУ «Институт стандартизации», 2023

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения 2
5 Соответствие типовой архитектуре ИВ 3
6 Цели и задачи типовой архитектуры системы ИВ 3
6.1 Общие положения 3
6.2 Характеристики 3
6.3 Концептуальная модель 4
6.4 Типовая модель и архитектурные представления 4
7 Характеристики систем ИВ 4
7.1 Общие положения 4
7.2 Характеристики доверенности системы ИВ 6
7.3 Характеристики архитектуры системы ИВ 8
7.4 Функциональные характеристики системы ИВ 13
8 Концептуальная модель ИВ 19
8.1 Основная задача 19
8.2 Понятия концептуальной модели ИВ 19
8.3 Высокоуровневое представление концептуальной модели 26
9 Типовая модель ИВ 28
9.1 *Общие положения* 28
9.2 Типовая модель ИВ 28
10 Представления типовой архитектуры ИВ 32
10.1 Общее описание 32
10.2 Функциональное представление типовой архитектуры ИВ 32
10.3 Представление развертывания системы типовой архитектуры ИВ 36
10.4 Сетевое представление типовой архитектуры ИВ 38
10.5 Представление использования типовой архитектуры ИВ 40
11 Доверенность системы ИВ 47
11.1 Общие положения 47
11.2 Безопасность 48
11.3 Защищенность 49
11.4 Приватность и защита персональных данных 50
11.5 Надежность 50
11.6 Способность к восстановлению 51
11.7 Доверенность и типовая архитектура 52
Приложение А (справочное) Интерпретация диаграммы классов UML для концептуальной модели . . . 54
Приложение В (справочное) Отношения сущностей концептуальной модели 55
Приложение С (справочное) Отношение между концептуальной моделью, типовой моделью и типовой архитектурой 59
Библиография 60

Введение

В настоящее время Интернет вещей (ИВ) широко применяется в промышленности и обществе, его развитие будет продолжаться в течение многих лет. Различные ИВ-приложения и службы, использующие методы ИВ, обеспечивают возможности, которые были недоступными еще несколько лет назад. Интернет вещей является одной из наиболее динамичных и перспективных информационно-коммуникационных технологий. ИВ подключает физические сущности («вещи») к ИТ-системам через сети. Основой интернета вещей являются электронные устройства, которые взаимодействуют с физическим реальным миром. Датчики собирают информацию о физическом мире, а исполнительные устройства могут оказывать воздействие на физические сущности. Датчики и исполнительные устройства могут иметь различные формы, например термометры, акселерометры, видеокамеры, микрофоны, реле, обогреватели или промышленное оборудование для производства или контроля процесса. Для сбора и обработки данных используются такие технологии как мобильные технологии, облачные вычисления, большие данные и глубокая аналитика (предиктивная, когнитивная, в режиме реального времени и контекстная). Данные предоставляют контекстную, актуальную и прогностическую информацию, которая оказывает влияние на физические и виртуальные сущности, что в конечном итоге позволяет контролировать физические сущности.

Технология ИВ может быть интегрирована в существующие технологии. Добавление датчиков к существующей технологии обеспечит проведение измерений текущего состояния, что способствует усовершенствованию существующей функциональности и снижению эксплуатационных расходов (например, умные светофоры адаптируются к дорожной обстановке, снижая перегруженность на дорогах и загрязнение воздуха). Данные, генерируемые ИВ-датчиками, могут поддерживать новые бизнес-модели и адаптировать товары и услуги к пониманию и потребностям заказчика. Помимо приложений, технологии необходимо поддерживать контроль над самой системой ИВ и ее адаптацию.

Возможные применения ИВ включают в себя такие области как умный город, интеллектуальные энергосети, умный дом/здание, цифровое сельское хозяйство, умное производство, интеллектуальные транспортные системы, электронное здравоохранение. ИВ является инновационной технологией, которая включает в себя поддерживающие технологии, например различные сетевые технологии, информационные технологии, технологии зондирования и контроля, программные технологии, приборные/аппаратные технологии.

Важным аспектом является доверенность, для ее обеспечения в интернете вещей необходимо использовать существующие и будущие передовые практики. Для поддержания надежности, безопасности и защищенности имеет важное значение мониторинг и анализ развернутых систем ИВ. Защищенность системы обеспечивают такие меры, как контролируемый доступ.

Настоящий стандарт определяет типовую архитектуру ИВ с единым подходом, повторно используемыми решениями и промышленными рекомендациями. В типовой архитектуре ИВ используется нисходящее проектирование, начиная со сбора наиболее важных характеристик интернета вещей, их абстрагирования в общую концептуальную ИВ-модель, получения типовой высокоуровневой модели и заканчивая определением четырех архитектурных представлений (функциональное представление, системное представление, сетевое представление и представление использования) типовой модели.

Типовая архитектура ИВ служит базой для разработки (специфицирования) контекстных конкретных архитектур ИВ и, следовательно, для реальных систем. Контексты могут быть различными, но должны включать в себя бизнес-контекст, регуляторный и технологический контекст, например отраслевые вертикали, технологические требования и/или наборы национальных конкретных требований (см. рисунок 1).

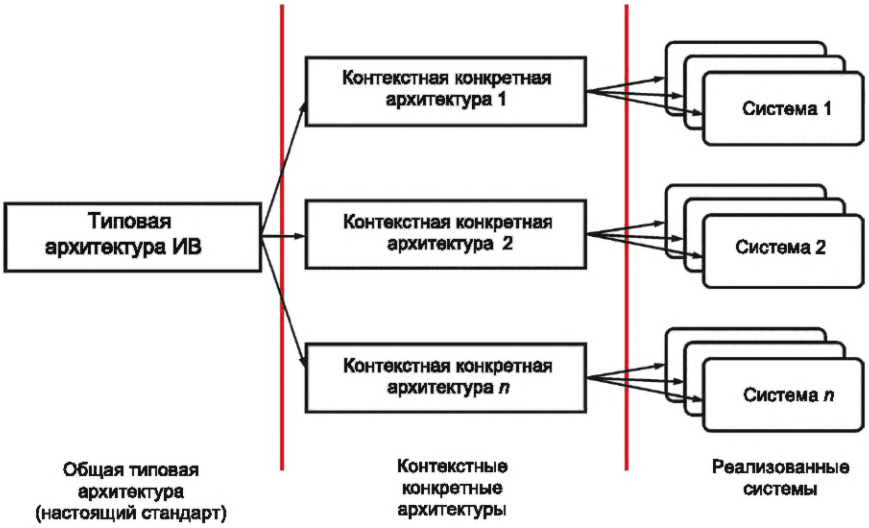

Рисунок 1 — Разработка систем ИВ с использованием типовой архитектуры

Вопросы безопасности выходят за рамки положений настоящего стандарта и являются объектом стандартизации профильных национальных технических комитетов.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ИНТЕРНЕТ ВЕЩЕЙ

Типовая архитектура

Information technology.
Internet of things.
Reference architecture

Дата введения — 2024—01—01

1 Область применения

Настоящий стандарт определяет общую типовую архитектуру Интернета вещей (ИВ) путем определения системных характеристик, концептуальной модели, типовой модели и архитектурных представлений.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 27.303 (МЭК 60812:2018) Менеджмент риска. Метод анализа видов и последствий отказов

ГОСТ Р 51901.5 (МЭК 60300-3-1:2003) Менеджмент риска. Руководство по применению методов анализа надежности

ГОСТ Р 56923/ISO/IEC TR 24748-3:2011 Информационные технологии. Системная и программная инженерия. Управление жизненным циклом. Часть 3. Руководство по применению ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)

ГОСТ Р 57100/ISO/IEC/IEEE 42010:2011 Системная и программная инженерия. Описание архитектуры

ГОСТ Р 57102/ISO/IEC TR 24748-2:2011 Информационные технологии. Системная и программная инженерия. Управление жизненным циклом. Часть 2. Руководство по применению ИСО/МЭК 15288

ГОСТ Р 57193 Системная и программная инженерия. Процессы жизненного цикла систем

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств

ГОСТ Р ИСО/МЭК 27000 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

ГОСТ Р ИСО/МЭК 27031 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса

ГОСТ Р ИСО/МЭК 27034-1 Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия

Издание официальное

ГОСТ Р МЭК 60300-1 Менеджмент риска. Руководство по применению менеджмента надежности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по [1].

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ИТ — информационные технологии;
ОВиК — отопление, вентиляция и кондиционирование;
СМИБ — система менеджмента информационной безопасности;
ЧМИ — человеко-машинный интерфейс;
ADSL — асимметричная цифровая абонентская линия (Asymmetric Digital Subscriber Line);
API — прикладной программный интерфейс (Application Programming Interface);
ASIC — интегральная схема специального назначения (Application-specific Integrated Circuit);
ASD — домен приложений и служб (Application & Service Domain);
BSS — система поддержки бизнеса (Business Support Systems);
CPO — руководитель службы по вопросам приватности (Chief Privacy Officer);
CRM — управление взаимоотношениями с клиентами (Customer Relationship Management);
DPO — специалист по защите данных (Data Protection Officer);
FQDN — полностью определенное имя домена (Fully Qualitied Domain Name);
HTTP — протокол передачи гипертекста (Hypertext Transfer Protocol);
IaaS — инфраструктура как услуга (Infrastructure as a Service);
IP — Интернет-протокол (Internet Protocol);
ISC — меры и средства контроля и управления защищенности системы ИВ (IoT system Security Controls);
KPI — ключевые показатели эффективности (Key Performance Indicators);
LOB — бизнес-линия (Line of Business);
MAC — управление доступом к мультимедиа (Media Access Control);
OID — идентификатор объекта (Object Identifier);
OMD — домен эксплуатации и управления (Operation & Management Domain);
OSS — система эксплуатационной поддержки (Operational Support Systems);
PaaS — платформа как услуга (Platform as a Service);
PED — домен физических сущностей (Physical Entity Domain);
PIA — оценка воздействия на приватность (Privacy Impact Assessment);
RAID — домен доступа и обмена ресурсами (Resource Access & Interchange Domain);
REST — передача состояния представления (Representational State Transfer);
RFID — радиочастотная идентификация (Radio-frequency Identification);
SaaS — программное обеспечение как услуга (Software as a Service);

SLA — Соглашение об уровне качества (Service Level Agreement);
SCD — домен восприятия и контроля (Sensing & Controlling Domain);
UML — унифицированный язык моделирования (Universal Modelling Language);
UD — домен пользователей (User Domain);
URI — унифицированный идентификатор ресурсов (Uniform Resource Identifier);
UUID — универсальный уникальный идентификатор (Universally Unique Identifier).

5 Соответствие типовой архитектуре ИВ

Архитектура системы ИВ соответствует настоящему стандарту, если в описании архитектуры системы, предоставляемой поставщиком или системным интегратором, использована терминология и концепция моделирования, определенные в настоящем стандарте.

6 Цели и задачи типовой архитектуры системы ИВ

6.1 Общие положения

Типовая архитектура системы ИВ определяет общие характеристики системы ИВ, концептуальную модель, типовую модель и ряд архитектурных представлений, согласованных с описаниями архитектуры по *ГОСТ Р 57100*. Общий структурированный подход к построению систем ИВ должен заключаться в определении структуры архитектуры. Типовая архитектура системы ИВ предоставляет рекомендации для архитектора по разработке системы ИВ и предназначена для заинтересованных сторон систем ИВ, включая производителей устройств, разработчиков приложений, клиентов и пользователей.

Настоящий стандарт определяет:

- общие ожидаемые характеристики систем ИВ;
- концептуальную модель, определяющую ключевые понятия системы ИВ;
- типовую модель, определяющую общую структуру элементов архитектуры;
- набор соответствующих архитектурных представлений с нескольких точек зрения.

На рисунке 2 показана типовая архитектура системы ИВ, которая включает в себя концептуальную модель, характеристики, типовую модель и одно или несколько архитектурных представлений.

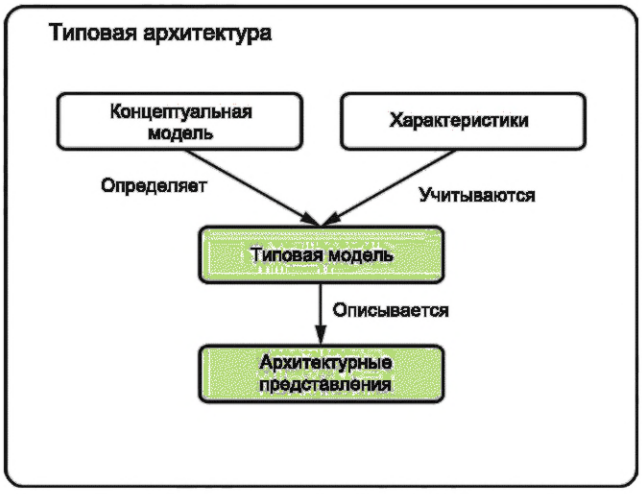

Рисунок 2 — Структура типовой архитектуры системы ИВ

6.2 Характеристики

Общие характеристики, которые отражают ключевые свойства системы ИВ, определены в разделе 7. Фактическое количественное представление характеристик различается для разных приложений, при разработке системы архитектор ИВ должен учесть, насколько важными являются соответствующие категории для конкретной разрабатываемой системы.

6.3 Концептуальная модель

Концептуальная модель определяет понятия и их логическую взаимосвязь. Концептуальная модель и общие характеристики представляют собой основу и обоснование для архитектурных элементов архитектурных представлений, определенных в разделе 10. Концептуальная модель определена в разделе 8.

6.4 Типовая модель и архитектурные представления

Типовая модель определена в разделе 9. Типовая модель и архитектурные представления показаны на рисунке 3.

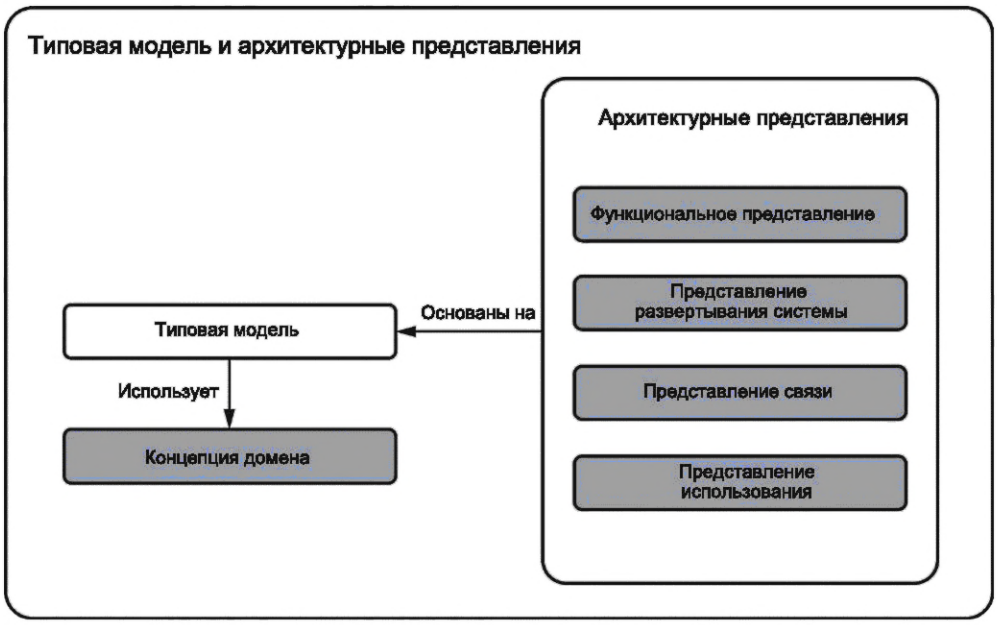

Рисунок 3 — Типовая модель и архитектурные представления

На рисунке 3 показана взаимосвязь между архитектурными представлениями, типовой моделью и концепцией домена. Концепция домена определена в концептуальной модели в 8.2.1.1 и 8.2.1.3. Типовая архитектура также использует концепцию домена. Подробное описание типовой архитектуры на основе домена представлено в 9.2.2.

Архитектурные представления определены в разделе 10.

7 Характеристики систем ИВ

7.1 Общие положения

В настоящем разделе определены характеристики систем ИВ. Функции, основанные на всех или части этих характеристик, могут быть реализованы в системах ИВ. Некоторые характеристики, например подключаемость сети, являются функциональными, другие — нефункциональными, например доступность и соответствие. Классификация и перечень характеристик представлены в таблице 1.

Таблица 1 — Характеристики систем ИВ

Классификация	Характеристика
7.2 Характеристики доверенности системы ИВ	7.2.2 Доступность
	7.2.3 Конфиденциальность
	7.2.4 Целостность
	7.2.5 Защита персональных данных
	7.2.6 Достоверность
	7.2.7 Способность к восстановлению
	7.2.8 Безопасность
7.3 Характеристики архитектуры системы ИВ	7.3.1 Компонуемость
	7.3.2 Разделение функциональных возможностей и возможностей управления
	7.3.3 Неоднородность
	7.3.4 Сильно распределенные системы
	7.3.5 Поддержка устаревших компонентов
	7.3.6 Модульность
	7.3.7 Подключаемость сети
	7.3.8 Масштабируемость
	7.3.9 Возможность совместного использования
	7.3.10 Уникальная идентификация
	7.3.11 Четко определенные компоненты
7.4 Функциональные характеристики системы ИВ	7.4.1 Точность
	7.4.2 Автоматическое конфигурирование
	7.4.3 Соответствие нормативным требованиям
	7.4.4 Информированность о контенте
	7.4.5 Информированность о контексте
	7.4.6 Характеристики данных: объем, скорость, достоверность, изменчивость и разнообразие
	7.4.7 Обнаруживаемость
	7.4.8 Гибкость
	7.4.9 Управляемость
	7.4.10 Сетевая связь
	7.4.11 Управление и эксплуатация сети
	7.4.12 Способность работы в режиме реального времени
	7.4.13 Самоописание
	7.4.14 Подписка на службу

7.2 Характеристики доверенности системы ИВ

7.2.1 Общие положения

Доверенность определяется как степень доверия к тому, что система работает согласно ожиданиям с такими свойствами, как безопасность, защищенность, приватность, надежность и способность к восстановлению в условиях воздействия окружающей среды, ошибок персонала, системных сбоев и атак.

В рамках положений настоящего стандарта защищенность определяется как совокупность доступности, конфиденциальности и целостности.

7.2.2 Доступность

7.2.2.1 Определение

Согласно ГОСТ Р ИСО/МЭК 27000 доступность — это свойство быть доступным и готовым к использованию по запросу авторизованной сущности. В системах ИВ авторизованными сущностями могут быть как пользователи, так и компоненты служб.

7.2.2.2 Роль в системах ИВ

В системах ИВ доступность рассматривается как характеристика устройств, данных и служб. Доступность устройства связана с его внутренними свойствами корректной работы на протяжении времени и с сетевой подключаемостью устройства. Доступность данных связана со способностью системы осуществлять прием/передачу требуемых данных из системного компонента или в него. Доступность служб связана со способностью системы предоставлять запрошенную службу пользователям с предварительно определенным качеством обслуживания.

7.2.2.3 Примеры

В некоторых критических приложениях, например в мониторинге работоспособности или обнаружении вторжений, доступность устройств и данных должна быть максимальной, чтобы сигналы тревоги могли быть отправлены в систему сразу при их возникновении. При проектировании системы должны быть учтены возможные варианты отказов и обеспечены средства продолжения функционирования, такие как резервирование источников питания, резервные устройства и несколько экземпляров службы.

7.2.3 Конфиденциальность

7.2.3.1 Определение

Согласно ГОСТ Р ИСО/МЭК 27000, конфиденциальность — это свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов.

7.2.3.2 Роль в системах ИВ

В системе ИВ политика и механизмы защиты конфиденциальности реализуют запрет чтения данных или управляющих сообщений для неавторизованных людей или систем.

Конфиденциальность является необходимым условием для безопасной работы, особенно когда передаваемые данные содержат секретные токены, например для контроля доступа. Конфиденциальность также требуется для защиты конфиденциальных данных, которые могут включать в себя персональные данные, например информацию о личном здоровье и финансовую информацию.

7.2.3.3 Примеры

Данные, проходящие через систему ИВ, могут считаться конфиденциальными. Конфиденциальные данные должны быть защищены от использования в преступных целях. Должно быть предотвращено ненадлежащее использование персональных данных. Например, по данным датчика обнаружения движения ИВ может быть определено, занят целевой объект или нет, что позволит злоумышленникам проникнуть на целевой объект.

В случае интеллектуальных счетчиков ИВ частота передаваемых сообщений не должна зависеть от потребляемой мощности, поскольку по этим данным может быть определено, занят целевой объект или нет.

7.2.4 Целостность

7.2.4.1 Определение

Согласно ГОСТ Р ИСО/МЭК 27000, целостность — это свойство сохранения правильности и полноты активов. Данная характеристика обычно применяется к информации внутри системы.

7.2.4.2 Роль в системах ИВ

Целостность является критически важной характеристикой систем ИВ. Данные, используемые для процессов принятия решений в системе и исполняемом программном обеспечении, не должны быть изменены неисправными или неавторизованными устройствами, злоумышленниками или условиями окружающей среды.

7.2.4.3 Примеры

При развертывании системы ИВ существует риск изменения данных промежуточным устройством, что влияет на функционирование системы. Например, в процессе обработки информации, промежуточный узел при обработке показаний о температуре и влажности в помещении не передал показания о влажности. В результате чего регулятор влажности оказался без сигнала обратной связи и перешел в неработоспособное состояние.

7.2.5 Защита персональных данных

7.2.5.1 Определение

Концепция защиты персональных данных частично пересекается, но не совпадает полностью с концепцией приватности. В системах ИВ сущности могут включать в себя людей, технологии и процессы.

В настоящем стандарте применено следующее определение термина «персональные данные»: «любая информация, которая может быть использована для идентификации владельца персональных данных, к которому относится такая информация, или прямо или косвенно связана с владельцем персональных данных».

Защита персональных данных должна быть обеспечена в случае, когда система ИВ на любом этапе работы включает в себя персональные данные. Это относится ко всем персональным данным, из которых могут быть получены, например путем агрегации, анализом или другими средствами, информативные персональные данные. Принцип минимизации данных устанавливает, что организации должны обрабатывать только минимально необходимые для определенных целей персональные данные. Персональные данные должны быть удалены, когда больше не требуются.

7.2.5.2 Роль в системах ИВ

Любая система ИВ, которая собирает, получает, обрабатывает и/или осуществляет обмен персональными данными, должна обеспечить полное соответствие таких систем ИВ и их взаимодействия с другими системами ИВ (или ИТ-системами в целом) требованиям защиты персональных данных.

7.2.5.3 Примеры

Независимо от сферы применения ИВ (например, носимые устройства, системы мониторинга здравоохранения, системы производства и строительства, автомобильная и энергетическая промышленность или «умные дома») владелец и оператор системы ИВ действуют как контроллер персональных данных и должны обеспечить, чтобы в системе ИВ были определены и реализованы необходимые элементы управления доступом и защитой данных.

7.2.6 Достоверность

7.2.6.1 Определение

Согласно ГОСТ Р ИСО/МЭК 27000, достоверность — это свойство соответствия предусмотренному поведению и результатам. Для соответствия системным требованиям должен быть обеспечен надлежащий уровень достоверности таких функциональных возможностей, как связь, обслуживание и управление данными.

Целевой уровень достоверности следует рассматривать в отношении риска, связанного с системой ИВ. Разработчик системы ИВ должен провести оценку риска. Оценка риска может быть проведена в соответствии с *ГОСТ Р 58771.*

7.2.6.2 Роль в системах ИВ

Необходимо обеспечить надлежащий уровень достоверности для различных вариантов развертывания системы и приложений ИВ. Достоверность является критическим параметром во всех системах управления с обратной связью.

7.2.6.3 Примеры

Достоверность данных имеет первостепенное значение для процессов принятия решений в большинстве систем ИВ. Отсутствие или искажение данных может привести к принятию неправильного решения или сбою принятия решения. Достоверность коммуникационных сетей обеспечивает доступность и корректную работу систем ИВ, особенно в критически важных системах или приложениях.

Пример — Промежуточный узел в процессе обработки внес изменения в измеренное значение температуры, а система кондиционирования воздуха при этом начала использовать не реальное, а измененное значение температуры; что привело к невозможности поддержания заданной температуры.

7.2.7 Способность к восстановлению

7.2.7.1 Определение

Способность к восстановлению — это способность системы ИВ или ее компонентов гибко адаптироваться и продолжать функционировать при наличии ошибок, неисправностей и других случайных изменений без потери уровня функционирования и производительности.

7.2.7.2 Роль в системах ИВ

В системах ИВ следует предусмотреть сбои связи, устройств или программных компонентов, которые без надлежащего проектирования могут вызвать глобальный сбой системы. Системы ИВ должны быть спроектированы для обеспечения способности к восстановлению, в том числе с использованием методов самоконтроля и самовосстановления для повышения устойчивости системы.

7.2.7.3 Примеры

Система ИВ должна иметь способность к восстановлению при сбоях в работе шлюзов для обеспечения постоянных каналов связи между компонентами программного обеспечения и устройствами ИВ.

Одним из методов обеспечения способности к восстановлению является добавление резервных устройств и линий связи в схему «ведущий — ведомый» (master-slave), в соответствии с которой в случае отказа главного устройства имеется резервное устройство для выполнения роли ведущего или резервируются ведомые устройства.

Для сетей структура ячеистой сети обладает способностью к восстановлению при отказе одного канала или одного узла, так как данные могут передаваться из источника в сток по альтернативному маршруту.

Способность к восстановлению можно сравнить с отказоустойчивым режимом компьютера или аварийным режимом автомобиля. Могут быть выполнены основные функции, но полная функциональность невозможна.

7.2.8 Безопасность

7.2.8.1 Определение

Безопасность — это состояние, в котором риск нанесения вреда (лицу) или ущерба ограничен до приемлемого уровня. Риск определяется вероятностью причинения вреда и тяжестью этого вреда. Вред включает в себя травмы или ущерб здоровью людей и ущерб имуществу или окружающей среде. Вред может быть вызван неисправностью, ошибкой или несчастным случаем. Вышеуказанные характеристики описывают требуемое поведение системы при правильной эксплуатации, безопасность же включает в себя рассмотрение видов неисправности с целью предотвращения, сокращения или смягчения возможности возникновения нежелательных результатов; в частности, ущерба, вреда или убытков.

7.2.8.2 Роль в системах ИВ

Многие системы ИВ разворачиваются в таких областях применения или эксплуатационных условиях, при которых может возникнуть ущерб, потери, травмы или смерть вследствие неправильного решения проблем неисправностей. Во многих эксплуатационных условиях разрешение на эксплуатацию или разрешение на подключение не выдаются, если не выполняются требования к безопасности.

Даже в областях применения, в которых соблюдение стандартов безопасности является необязательным, надлежащий учет факторов безопасности имеет значительное влияние на такие аспекты как: повреждение оборудования, предотвращение травм или смерти, страховые премии, правонарушения и ответственность и т. д.

7.2.8.3 Примеры

Области применения систем ИВ, в которых требуется учитывать стандарты или требования безопасности, включают в себя промышленность, медицину, транспортные перевозки (авиация и автомобильная индустрия), товары широкого потребления, строительство и мониторинг окружающей среды. Большинство стран устанавливает нормативные требования, касающиеся таких областей применения, как например, пожарная безопасность, безопасность национальных границ, мониторинг радиационных повреждений в больницах и центрах ядерных исследований.

7.3 Характеристики архитектуры системы ИВ

7.3.1 Компонуемость

7.3.1.1 Определение

Компонуемость — это способность объединять отдельные компоненты ИВ в систему ИВ для достижения ряда целей и задач.

7.3.1.2 Роль в системах ИВ

Системная интеграция, функциональная совместимость и компонуемость определяют, как функциональные компоненты собираются в единую систему ИВ, как функциональные компоненты соединяются друг с другом, и какие механизмы связывания используются (например, динамический или статический, агентный или одноранговый). Функциональная совместимость и компонуемость являются важными аспектами в кибер- и физическом пространствах. Компонуемость налагает более строгие требования, чем функциональная совместимость, так как компонуемость требует не только совместимости компонентов с их интерфейсами, но и взаимозаменяемости с другими компонентами того же рода. Как минимум, эти компоненты имеют схожую конструкцию и улучшенные характеристики, такие как время, производительность, масштабируемость и защищенность. Когда компонент заменяется другим аналогичным совместимым компонентом, общие функции и характеристики системы, как минимум, должны оставаться неизменными, но может быть разрешено внесение улучшений в функции и характеристики системы.

7.3.1.3 Примеры

Одним из примеров компонуемости является датчик температуры в офисном здании с четко определенными возможностями и стандартизированным интерфейсом служб. Датчик температуры может быть интегрирован в систему ОВиК и использоваться в управлении температурой комнаты и здания. Также датчик может быть интегрирован в систему аварийного реагирования для случая пожарной тревоги и предоставлять данные сотрудникам службы реагирования о комнатах с источником огня.

Вторым уровнем компонуемости (или, возможно, функциональной совместимости) может быть контроллер ИВ. Контроллер ИВ зависит от поставщика на интерфейсе между компонентом ИВ и управляемым физическим устройством процесса (например, клапаном, двигателем, переключателем, насосом или вентилятором), но является полностью заменяемым на интерфейсе между устройством ИВ и остальной частью системы ИВ. В данном примере устройство ИВ будет своего рода «промежуточным программным обеспечением» между независимой от поставщика инфраструктурой ИВ и управляемыми физическими устройствами или механизмами конкретного поставщика.

7.3.2 Разделение функциональных возможностей и возможностей управления

7.3.2.1 Определение

Разделение функциональных возможностей и возможностей управления означает, что функциональные интерфейсы и возможности ИВ-компонента (например, ИВ-устройства) однозначно отделяются от интерфейсов и возможностей управления данного компонента. Как правило, это означает, что интерфейс управления находится на оконечной точке, отличной от оконечной точки функционального интерфейса, а возможности управления обрабатываются программными компонентами, отличными от программных компонентов, обрабатывающих функциональные интерфейсы.

7.3.2.2 Роль в системах ИВ

Возможности управления и функциональные возможности имеют логически разные:

- цели (выполнение/действие либо информация/описание);
- роли пользователей (режим контроля и внесения изменений либо факты и информация о передачах и потреблении);
- классификацию и типы данных (технические данные или данные о системе либо персональные/информативные/общедоступные данные);
- доступ (например, оператор может получить доступ к настройке системы, но не к собранным персональным данным; либо пользователь может получить доступ к персональным данным, но не к изменению настроек системы);
- протоколы, форматы и жизненные циклы (например, поддержка множества протоколов контроля либо метаданные/структура передаваемой информации, что особенно важно с учетом функциональной совместимости и сосуществования нескольких версий и вариантов управленческих возможностей).

Как правило, различия в возможностях приводят к различиям в рисках и, следовательно, требуют различный контроль безопасности. Например, политика хранения при работе с функциональными данными может не применяться к данным управления, контроль доступа может быть менее строгим для пользователя и строгим для администратора.

Повсеместное распространение ИВ практически во всех сферах жизни увеличивает поверхность атаки, увеличивает число потенциальных целей атаки и часто делает неэффективными такие меры, как контроль физической безопасности. Ключевой особенностью ИВ является соединение многочисленных периферийных компонентов друг с другом и с компонентами службы ИВ. Это увеличивает проблемы безопасности, поскольку добавление слабого звена делает всю цепочку слабой. Приложения и систе-

мы, ранее работавшие в хорошо защищенных центрах обработки данных, могут подвергаться дополнительным угрозам через подключенные компоненты ИВ.

Отделение возможностей управления от функциональных возможностей обеспечивает или усиливает возможность применения различных механизмов авторизации, аутентификации и защиты или ограничений к управлению в отличие от функциональных возможностей. Широкое совместное использование данных системы ИВ может быть полезным или требуемым, однако в некоторых случаях необходимо ограничить контроль системы или компонента ИВ только для подмножества сущностей, которым предоставлено совместное использование данных из системы ИВ.

7.3.2.3 Примеры

Для предоставления датчиков и данных системы ИВ для систем ОВиК или других систем управления зданием может требоваться совместное использование данными с другими взаимосвязанными системами (аварийные сигналы, управление доступом, управление питанием или дополнительное электропитание и т. д.). При этом управление системой обеспечивает соблюдение системных ограничений.

7.3.3 Неоднородность

7.3.3.1 Определение

Система ИВ, как правило, состоит из набора разнообразных компонентов и физических сущностей, которые взаимодействуют различными способами.

7.3.3.2 Роль в системах ИВ

Система ИВ, как правило, является межсистемной, межпродуктной и междоменной. Реализация полного потенциала ИВ требует взаимодействия неоднородных компонентов и систем. Неоднородность создает многочисленные проблемы для взаимосвязанных систем ИВ.

7.3.3.3 Примеры

Существуют различные промышленные коммуникационные технологии, что подразумевает различные неоднородные комбинации связи в подключенном производственном оборудовании, устройствах контроля и управления. Завод может иметь несколько производственных линий, которые расширяются по мере увеличения доходов от бизнеса. Постепенное расширение может увеличить разнообразие оконечных точек связи и, в конечном итоге, увеличит неоднородность всей системы.

7.3.4 Сильно распределенные системы

7.3.4.1 Определение

Распределенные системы являются функционально интегрированными и состоят из подсистем, которые могут быть физически отделены и удаленно расположены друг от друга. Подсистемы, как правило, соединены каналом связи (например, по шине передачи данных).

Сильно распределенные системы не обязательно являются стационарными во времени. Некоторые системы, такие как RFID-отслеживание, имеют высокую степень мобильности для отдельных устройств, что приводит к постоянно меняющейся топологии.

7.3.4.2 Роль в системах ИВ

Системы ИВ могут охватывать здания, города и весь мир. Может быть широкое распределение данных, которые могут храниться на периферии сети и/или централизованно. Распределение также может применяться к обработке: одна часть обработки проводится централизованно (в облачных сервисах), а другая часть — на периферии сети, шлюзах ИВ или даже внутри датчиков и исполнительных устройств.

7.3.4.3 Примеры

Для концепции «Индустрия 4.0» производство может включать в себя умные производственные системы с распределенными линиями сборки. Данные линии протягиваются через несколько предприятий и тесно интегрируются с удаленными поставщиками, логистическими компаниями, поставщиками и потребителями рынка, что представляет собой горизонтальную интеграцию.

7.3.5 Поддержка устаревших компонентов

7.3.5.1 Определение

Поддержка устаревших компонентов системой ИВ обозначает использование существующих установленных компонентов, даже если эти компоненты используют технологии, которые более не являются стандартными или утвержденными. Такими компонентами могут быть служба, протокол, устройство, система, компонент, технология или стандарт.

7.3.5.2 Роль в системах ИВ

Поддержка интеграции устаревших компонентов и миграции на новые версии имеют важное значение. Помимо поддержки устаревших компонентов структура новых компонентов и систем не должна иметь необоснованных ограничений для будущего развития системы. Во избежание нецелесообраз-

ного инвестирования в устаревшие компоненты, должен быть разработан план адаптации устаревших компонентов и миграции на новые версии. При интеграции устаревших компонентов должны быть обеспечены требования к защищенности, производительности и функциональности. Использование устаревших компонентов может увеличить риски и уязвимости. Поскольку современные технологии неизбежно устаревают, необходим процесс управления устаревшими компонентами ИВ. В системах ИВ разные подключенные устройства могут иметь разные жизненные циклы и расписание обновлений, что создает дополнительные трудности для управления устаревшими элементами ИВ.

7.3.5.3 Примеры

Одним из примеров перехода от устаревшего компонента с обеспечением совместимости является постепенный переход от требований четвертой версии интернет-протокола IPv4 к требованиям шестой версии интернет-протокола IPv6. Ограничения адресного пространства IPv4 и протокола IPv4 известны, и в будущем будет осуществлен переход к IPv6, но темп этого перехода постоянно меняется в зависимости от различных факторов и обстоятельств. Данный переход особенно актуален для ИВ с учетом большого количества устройств для подключения.

Многие существующие стандарты и прикладные среды поддерживают IPv4, однако бессрочное использование IPv4 является неэффективной стратегией. Причинами для перехода являются отсутствие достаточного адресного пространства и маскировка нескольких адресов за одним IP-адресом. Время перехода на IPv6 зависит от организации и зависит от множества факторов.

7.3.6 Модульность

7.3.6.1 Определение

Модульность — это свойство компонентов, которые могут быть объединены для формирования более крупных систем компонентов. Модульные компоненты могут быть аккуратно удалены из системы и заменены модулем аналогичного размера с аналогичными физическими и логическими интерфейсами.

7.3.6.2 Роль в системах ИВ

Модульность позволяет объединять компоненты в различных конфигурациях для формирования необходимых систем. Использование стандартизированных интерфейсов без определения внутренней работы каждого компонента обеспечивает разработчикам гибкость в проектировании компонентов и систем ИВ.

7.3.6.3 Примеры

Примером модульности в системе ИВ является «умный термостат». Если интерфейс для системы ОВиК и интерфейс для более крупной инфраструктуры ИВ определены в соответствии со стандартами открытого интерфейса, термостат от поставщика А может быть заменен на термостат от поставщика В. Способ реализации функциональности устройства не имеет значения. Поставщик А может использовать конечный автомат на основе ASIC, а поставщик В — микроконтроллер. Пока оба устройства выполняют аналогичные функции в ответ на аналогичные входные данные и совместимы с открытыми стандартными интерфейсами без проприетарных ограничений, препятствия для замены одного устройства другим отсутствуют.

7.3.7 Подключаемость сети

7.3.7.1 Определение

Основной концепцией ИВ являются сущности ИВ, способные поддерживать связь со многими другими сущностями по сети связи. Это отношение «многие ко многим» обеспечивает другие характеристики ИВ, в том числе компонуемость, способность к восстановлению, возможность совместного использования, масштабируемость и обнаружение, и в то же время создает проблемы в области защищенности, надежности, управляемости, точности, способности функционирования в режиме реального времени, приватности и безопасности. В системах ИВ компоненты взаимодействуют друг с другом через сетевые каналы. Связи между компонентами устанавливаются с помощью проводной или беспроводной среды. Сетевые устройства ИВ, которые инициируют, маршрутизируют и завершают связь, описываются как узлы (сетевые). Оконечные сетевые устройства являются источником или адресатом любой передаваемой информации. Протокол сетевого взаимодействия, связанный с ИВ, накладывается на более конкретные и более общие протоколы взаимодействия, вплоть до физического слоя, который непосредственно связан со средствами передачи на каждом сетевом узле.

7.3.7.2 Роль в системах ИВ

Системы ИВ основаны на структурированном обмене информацией с использованием множества разных, но способных взаимодействовать сетевых подключений внутри физической проводной или беспроводной сети. Устройства ИВ являются «сетевыми», когда одно устройство может обмениваться информацией с другими устройствами независимо от наличия прямого соединения между ними.

Структура сети ИВ может быть статической или динамической и иметь такие возможности, как качество обслуживания, способность к восстановлению, шифрование, аутентификация и авторизация.

7.3.7.3 Примеры

Масштаб сети ИВ может существенно различаться: от локальных сетей, соединяющих несколько устройств на ограниченном расстоянии, до глобальных сетей, работающих в масштабе Интернета и соединяющих очень большое количество устройств и компонентов уровня служб.

Как правило, сети в системах ИВ являются неоднородными и соединенными друг с другом через шлюзы или эквивалентные компоненты.

7.3.8 Масштабируемость

7.3.8.1 Определение

Масштабируемость — это свойство системы эффективно работать по мере увеличения размера системы, ее сложности или объема выполняемой работы.

7.3.8.2 Роль в системах ИВ

Системы ИВ включают в себя различные элементы, такие как устройства, сети, службы, приложения, пользователи, хранимые данные, трафик данных, отчеты о событиях. Количество каждого элемента может меняться со временем, и система ИВ должна эффективно функционировать при увеличении их количества.

7.3.8.3 Примеры

Примером масштабируемости является увеличение количества сенсорных устройств, подключенных к системе ИВ, за определенный период времени. При переходе системы от мониторинга датчиков температуры в одном здании к мониторингу датчиков температуры во всех зданиях в городе значительно увеличится объем сенсорных данных в системе, объем данных в базах данных, количество устройств, обрабатываемых системой управления, и количество показателей температуры, обрабатываемых службами и приложениями.

7.3.9 Возможность совместного использования

7.3.9.1 Определение

Возможность совместного использования — это возможность получить доступ к отдельному компоненту и его ресурсам, совместно распределяемым между несколькими взаимосвязанными системами.

7.3.9.2 Роль в системах ИВ

Многие ИВ-компоненты используются недостаточно эффективно, так как в одной системе обычно используется только малая часть возможностей компонента. Ресурсы могут использоваться более эффективно, если функциональность или выходные характеристики компонентов могут совместно использоваться несколькими системами.

7.3.9.3 Примеры

Функция обнаружения движения системы управления освещением может быть использована системой безопасности для увеличения возможностей системы безопасности.

Датчик температуры для контроля обогрева может быть использован системой безопасности для обнаружения пожара.

7.3.10 Уникальная идентификация

7.3.10.1 Определение

Уникальная идентификация — это свойство системы ИВ однозначно и повторяемо связывать сущности в системе с отдельным именем, кодом, символом или номером и взаимодействовать с сущностями, а также отслеживать или контролировать их деятельности с использованием ссылок на имя, код, символ или номер. Сущности включают в себя компоненты непосредственно системы ИВ, такие как компоненты программного обеспечения, датчики и исполнительные устройства, а также сетевые компоненты.

7.3.10.2 Роль в системах ИВ

Сущности в системе ИВ должны быть отличимы друг от друга. Это обеспечивает функциональную совместимость и глобальные службы в неоднородных системах ИВ. Сущности должны быть однозначно идентифицированы в заданном контексте, чтобы системы ИВ могли надлежащим образом отслеживать их и связываться с ними. Некоторые устройства могут быть скрыты за шлюзами ИВ или объединены для защиты приватности. В конкретных реализациях систем ИВ для удовлетворения требований приложения могут быть использованы различные схемы идентификации.

7.3.10.3 Примеры

IPv4-адрес, IPv6-адрес, MAC-адрес, URI и имена FQDN используются в качестве уникальной однозначной идентификации оконечных точек в соответствующем сетевом контексте. Отдельные аппа-

ратные устройства, программное обеспечение и другие сущности могут иметь уникальные идентификаторы производителя, идентификаторы объектов, универсальные уникальные идентификаторы (OID, UUID) или другие идентификаторы для уникальной идентификации.

Для физических сущностей используются метки в виде меток радиочастотной идентификации (RFID), штрих-коды и их эквиваленты. Данные носители содержат кодированные идентификаторы, которые могут распознаваться устройством ИВ. Уникальная идентификация человека может проводиться с использованием биометрической информации.

7.3.11 Четко определенные компоненты

7.3.11.1 Определение

Сущности ИВ считаются четко определенными, когда доступно точное описание их возможностей и характеристик, в том числе любые связанные с ними неопределенности. Информация о возможностях включает в себя информацию о функциональности компонента, конфигурации, связи, защищенности, надежности и другую соответствующую информацию.

7.3.11.2 Роль в системах ИВ

Для сборки системы ИВ используется множество компонентов. Как правило, они обнаруживаются через интерфейс информационной системы, и метаданные компонента могут быть недоступны из-за того, что компонент не соответствует стандарту или не способен хранить метаданные. Без понимания возможностей каждого используемого компонента усложняется определение того, отвечает ли система своей заданной цели.

7.3.11.3 Примеры

Пример реализации четко определенного компонента: определенный компонент ИВ доступен с различным количеством памяти или поддержкой различных радиочастот, форм кривых и протоколов. Устройство имеет базовый информационный интерфейс, который может быть использован для информирования других компонентов ИВ о перечне возможностей устройства. После обмена соответствующими конфигурациями устройств программное обеспечение или приложения каждого устройства могут самостоятельно настраиваться для учета возможностей других устройств.

7.4 Функциональные характеристики системы ИВ

7.4.1 Точность

7.4.1.1 Определение

Точность является характеристикой различных элементов в системе ИВ.

Датчики производят измерения свойств физического мира. Точность датчиков — это степень соответствия измеренных значений фактическим значениям свойств.

Программные службы могут проводить расчеты на основе входных данных. В случае программного обеспечения для автоматической обработки изображений (например, распознавание номерных знаков транспортных средств или распознавание лиц для идентификации людей) точность выражается в вероятности соответствия распознанного текста номерного знака фактическому или распознанного идентификатора человека фактическому.

Исполнительные устройства, функционирующие в физическом мире, преобразуют цифровые команды в действия. Точность исполнительных устройств может быть определена как степень соответствия фактических действий в физическом мире тем, которые предназначены цифровой командой. Примером может служить роботизированная рука, когда по цифровой команде должен быть перемещен конец роботизированной руки в определенное место в трехмерном пространстве. Точность определяется степенью соответствия фактического положения конца руки робота положению в цифровой команде.

В некоторых случаях точность выражается в отклонении цифрового значения аналоговой величины от ее истинного значения в физическом мире. В других случаях точность выражается как процент случаев, в которых цифровое значение соответствует ожидаемому значению (процент корректных значений).

7.4.1.2 Роль в системах ИВ

Для развертывания и приложений системы ИВ должен быть обеспечен соответствующий уровень точности. Требования к уровню точности определяются в зависимости от контекста.

7.4.1.3 Примеры

В области медицины или производства требования к точности измерения или контроля устройством, приложением или системой ИВ могут доходить до десятых долей градуса. Для домашней системы ОВиК достаточным является требование к точности в два градуса.

7.4.2 Автоматическое конфигурирование

7.4.2.1 Определение

Автоматическое конфигурирование устройств основано на взаимодействии предопределенных правил (связанных алгоритмов, основанных на вводе данных). Автоматическое конфигурирование включает в себя автоматическую организацию сети, автоматическое предоставление служб и технологию «plug and play» («включил и играй»). Автоматическое конфигурирование позволяет системе ИВ реагировать на условия, добавлять и удалять компоненты, такие как устройства и сети. Автоматическое конфигурирование требует механизмов защиты и аутентификации для гарантии того, что только авторизованные компоненты могут быть автоматически настроены в системе. Механизмы защиты должны быть организованы соответствующим образом для каждого сегмента рынка.

7.4.2.2 Роль в системах ИВ

Автоматическое конфигурирование целесообразно для систем ИВ с большим количеством различных компонентов, которые могут меняться на протяжении времени. Устранение неисправных компонентов и своевременное техническое обслуживание, проводимое с использованием автоматического конфигурирования, повышает надежность системы.

7.4.3 Соответствие нормативным требованиям

7.4.3.1 Описание

Системы, службы, компоненты и приложения ИВ могут быть развернуты в условиях, которые требуют соблюдения ряда нормативно-правовых документов. Устройства или системы ИВ могут соответствовать нормативным требованиям, или для обеспечения соответствия потребуются определенная конфигурация, программирование, модификация или расширение.

Может существовать диапазон различной степени детализации или уровней абстракции, на которых применяются правила (или требуется их соблюдение).

7.4.3.2 Роль в системах ИВ

Нормативные требования к системе ИВ могут обеспечивать функциональную совместимость, предписывать или ограничивать функциональность или возможности, оценивать способность устройства или системы ИВ функционировать при условии соблюдения требований без причинения ущерба, а также обеспечивать баланс между вкладом в общественные блага и личными интересами владельцев и операторов системы.

7.4.3.3 Примеры

Примеры требований в области ИВ:

а) требования к безопасности. Например, стандарты обеспечения безопасности для устройств ИВ, используемых в авиатранспорте, требования к производству и продаже устройств для домашнего использования, требования к автомобильным системам или требования для медицинских устройств или систем;

б) требования к радиочастотам. Например, национальные или международные нормативы, регулирующие излучение РЧ, соблюдение ограничений полосы частот, уровня сигнала, сигналов помехи (таких как боковые каналы, шум или гармоники, возникающие за пределами номинального распределения частот устройства);

в) требования к защите потребителей. Например, национальные и международные нормативы, касающиеся потребителя в работе системы ИВ.

В некоторых контекстах ИВ, таких как домашняя автоматизация и ОВиК, в различных юрисдикциях нормативные требования могут быть введены в виде строительных норм и правил.

В будущем возможна ситуация, когда страховые компании будут применять правила или ссылаться на них как на часть своих моделей риска для расчета цен на конструкции, транспортные средства, системы или предприятия, использующие системы и устройства ИВ.

7.4.4 Информированность о контенте

7.4.4.1 Определение

Информированность о контенте — это свойство наличия достаточных знаний об информации в компоненте ИВ и связанных метаданных. Устройства и службы с информированностью о контенте способны адаптировать интерфейсы, абстрагировать данные приложений, повысить точность поиска информации, обнаружить службы и обеспечить соответствующее взаимодействие с пользователем.

7.4.4.2 Роль в системах ИВ

Информированность о контенте упрощает соответствующие функциональные операции, такие как маршрутизация данных, скорость доставки, возможности защищенности, такие как шифрование на основе факторов местоположения, требований к качеству службы и чувствительности данных.

7.4.4.3 Примеры

Информированность о контенте имеет важное значение для многих приложений, включая медицинское обслуживание, вещание, системы наблюдения и аварийно-спасательные службы, в которых некоторые типы потоков информации или данных имеют требования к своевременности, защищенности и приватности.

7.4.5 Информированность о контексте

7.4.5.1 Определение

Информированность о контексте — это свойство устройства, службы или системы ИВ, которые могут отслеживать свою собственную среду эксплуатации и события в данной среде для определения информации, когда (осведомленность о времени), где (осведомленность о местоположении) или в каком порядке (осведомленность о последовательности событий) одно или несколько наблюдений произошли в физическом мире.

7.4.5.2 Роль в системах ИВ

Информированность о контексте обеспечивает гибкие, настраиваемые пользователем и автономные службы на основе соответствующего контекста компонентов ИВ и/или пользователей. Информация о контексте используется для принятия решения по наблюдению, возможно, путем использования сенсорной информации и исполнительных устройств. Понимание контекста часто имеет решающее значение для полного использования данных наблюдения и совершения действия.

7.4.5.3 Примеры

Примером являются службы, основанные на определении местоположения, такие как система, в которой различные службы представляются в зависимости от местоположения пользователя.

В случае возникновения чрезвычайной ситуации, такой как пожар, прибытие пожарной службы требует, чтобы двери в здание были разблокированы. Политика безопасности, которая регулирует доступ к двери, может быть дополнена информацией о контексте. В данной ситуации контекстом является чрезвычайная ситуация в настоящее время и близкое расположение аварийно-спасательных служб. На основании указанных входных данных о контексте, политика доступа может автоматически активировать систему разблокировки двери и обеспечить доступ без необходимости дальнейшей авторизации.

7.4.6 Характеристики данных: объем, скорость, достоверность, изменчивость и разнообразие

7.4.6.1 Определение

Характеристики данных: объем, скорость, достоверность, изменчивость и разнообразие* заимствованы из области больших данных. Это обусловлено тем, что системы ИВ являются источником данных, больших по объему, которые доставляются с высокой скоростью по сетевым каналам, чья достоверность должна быть проверена (например, из-за неисправности датчиков), которые могут изменяться на протяжении времени и могут содержать различные типы данных из различных компонентов ИВ.

7.4.6.2 Роль в системах ИВ

В системах ИВ образуется большое количество данных из различных местоположений. Данные могут быть объединены в централизованных месторасположениях или могут быть сохранены в распределенных месторасположениях (в зависимости от характера данных, требуемой обработки данных и характеристик канала связи), что вызывает необходимость надлежащим образом индексировать, хранить, обрабатывать и защитить данные.

7.4.6.3 Примеры

Логистическая компания использует анализ больших данных для службы комплексной оптимизации и навигации на дорогах. Система использует многочисленные адресные точки данных, а также другие данные, собранные в процессе доставки грузов, для оптимизации маршрутов доставки.

7.4.7 Обнаруживаемость

7.4.7.1 Определение

Обнаруживаемость является свойством оконечной точки сети, которая определяется динамически и сообщает о своих службах и их возможностях через подходящий механизм запросов или меха-

* В англоязычных документах указанные характеристики называются «5V» (volume, velocity, veracity, variability, variety).

низм саморекламы. Оконечными точками могут быть устройства, службы и приложения ИВ или даже пользователи. Соответствующие службы обнаружения позволяют обнаруживать, идентифицировать и получать доступ к оконечным точкам в соответствии с изменяемыми критериями, такими как географическое местоположение или тип службы.

7.4.7.2 Роль в системах ИВ

Службы, связанные с системой ИВ, могут указывать, какую информацию можно найти с помощью службы обнаружения/поиска в соответствии с предопределенными правилами для каждого сегмента рынка. Службы обнаружения/поиска позволяют системам ИВ обнаруживать другие устройства, службы или системы на основе таких параметров, как географическое положение, возможности, интерфейсы, доступность, право собственности, политика безопасности, эксплуатационная конфигурация, или другие соответствующие факторы.

7.4.7.3 Пример

Системы ИВ с поддержкой динамической конфигурации, например добавления новых устройств и служб в систему ИВ, имеют некоторые требования к обнаруживаемости, поскольку существует необходимость определить и охарактеризовать новые компоненты, добавленные в систему. Примером является добавление нового датчика температуры в систему ИВ мониторинга здания, когда необходимо ввести новый датчик в существующую систему с минимальными усилиями. Для обеспечения обнаруживаемости в системах ИВ существуют различные протоколы и программные решения со множеством архитектур. Некоторые архитектуры являются серверными, другие — одноранговыми.

7.4.8 Гибкость

7.4.8.1 Определение

Гибкость — это свойство системы, службы, устройства или другого компонента ИВ предоставлять различную функциональность в зависимости от потребности или контекста.

7.4.8.2 Роль в системах ИВ

Несмотря на исключения, как правило, экономическая и функциональная оптимальная точка гибкости находится посередине между крайними точками. Одной крайней точкой является одноцелевой специализированный компонент. Второй крайней точкой является многофункциональный, программируемый, расширяемый компонент общего назначения «все для всех».

Гибкость по отношению к ИВ имеет разные аспекты.

Гибкость системы ИВ обусловлена возможностью соединять службы ИВ различными способами, динамически и во время выполнения. Хотя возможности каждой службы ИВ не меняются, при этом количество и разнообразие потенциальных систем очень велико.

Гибкость компонента ИВ иллюстрируется различием следующих категорий компонентов:

а) устройство с фиксированной, непрограммируемой, нерасширяемой функциональностью — «жестко смонтированное, одноцелевое»;

б) устройство с фиксированными аппаратными возможностями, но с возможностями конфигурирования в рамках отдельного доступного формата;

в) устройство, которое является программируемым и расширяемым в области аппаратного обеспечения (например, добавление памяти, добавление дополнительных вычислительных возможностей или добавление возможностей радиочастотного канала);

г) семейство устройств, каждое из которых может быть отнесено к категориям, приведенным в перечислениях *а)—в)*, из которых интегратор выбирает одно или несколько устройств, подходящих для текущего контекста;

д) семейство устройств, как в категории *г)*, где опции на разных уровнях абстракции обеспечивают различную степень компонуемости или модульности.

Гибкость может включать в себя ряд стандартов, протоколов, форматов и интерфейсов, которые компонент ИВ должен поддерживать. Такая поддержка может разрабатываться и внедряться с учетом вышеуказанных факторов.

Существует еще один аспект гибкости, который включает в себя общую схему системы ИВ. Как и в других областях, предполагается наличие открытых и проприетарных экосистем ИВ.

7.4.8.3 Примеры

Примером различий гибкости датчика является термостат. Простейшие устройства обеспечивают контроль температуры и предоставление данных о температуре. Более сложные и гибкие термостаты предлагают дистанционное управление через смартфон, подключение к другим устройствам ИВ в здании для выявления заполняемости, получения информации о погоде и т. д. Более функциональные

устройства, как правило, имеют программные компоненты, которые могут быть модернизированы для обеспечения новых возможностей.

7.4.9 Управляемость

7.4.9.1 Определение

Управляемость включает в себя такие аспекты систем ИВ, как управление устройствами, управление сетью, управление системой, обслуживание интерфейса и оповещения. Управляемость необходима для удовлетворения требований системы ИВ. Для управляемости устройства, сети и системы ИВ необходимы компоненты, которые могут осуществлять контроль и вносить изменения в настройки.

7.4.9.2 Роль в системах ИВ

Многие устройства, сети и системы ИВ работают автономно. Такие системы должны оставаться управляемыми даже в случаях, когда части системы становятся неисправными, нестабильными или неправильно откалиброванными в ходе эксплуатации. Даже когда доступны отдельные сущности ИВ, потенциально крупномасштабный и географический охват систем ИВ требует максимально возможного удаленного управления сущностями ИВ для повышения удобства и эффективности работы.

7.4.9.3 Примеры

Устройства ИВ, такие как датчики дыма, устанавливаются в разных местах зданий, из-за чего могут возникнуть трудности в обслуживании. Любой тип неисправности может вызвать нежелательные события и последствия. Таким образом, удаленное управление должно учитываться в проекте системы и являться одной из основных задач проекта с начала составления спецификации, а также на протяжении разработки, развертывания и рабочего жизненного цикла системы ИВ.

Серверы обновлений встроенного программного обеспечения и репозитории операционной системы должны иметь возможность проверить подлинность компонента ИВ и наоборот (взаимная аутентификация). Обновления должны быть подписаны цифровой подписью для обеспечения их подлинности и целостности. Обновления должны передаваться по защищенному каналу при наличии возможности.

7.4.10 Сетевая связь

7.4.10.1 Определение

Системы ИВ зависят от множества типов сетей. Локальные соединения для устройств ИВ часто обеспечиваются сетями ближнего действия с малым энергопотреблением и с ограниченным радиусом действия. Существуют глобальные вычислительные сети, подсоединяющие сети ближнего действия к Интернету и которые могут быть проводными и беспроводными и предназначаться для системы ИВ или быть совместно используемыми сетями общего назначения.

Используемые протоколы связи определяются типом сети. Для сетей ближнего действия характерно использование специализированных протоколов с учетом особенностей конкретной сети. IP чаще используется для глобальных сетей, в этом случае могут различаться более высокие уровни в стеке протоколов, и в некоторых случаях используется HTTP, в других — протоколы обмена сообщениями. Некоторые сети являются преднамеренно прерывистыми по своему устройству, в этом случае используются протоколы, учитывающие модель прерывистой передачи.

7.4.10.2 Роль в системах ИВ

Системы ИВ рассчитаны на обмен информационными единицами структурированным способом по различным, но совместимым типам сетей. Устройства должны передавать и получать данные, а также поддерживать связь с программными службами, расположенными поблизости или в удаленном месте.

Для соединения сетей разных типов могут быть использованы шлюзы, как правило, между сетями ближнего действия и глобальными сетями. Структура сети может быть динамичной и должна учитывать такие свойства, как качество обслуживания, способность к восстановлению, защищенность и управляемость.

7.4.10.3 Примеры

В сети ближнего действия устройства ИВ могут быть подключены с помощью беспроводной технологии по протоколам связи на физическом и канальном уровнях. Передача данных может проводиться по стандарту 6LoWPAN, ориентированному на ИВ.

7.4.11 Управление и эксплуатация сети

7.4.11.1 Определение

Системы ИВ требуют управления сетью. Форма и назначение управления сетью и ее эксплуатации зависят от типа сети, формы собственности сети и типа сетевой связи. Управление требуется во время начального конфигурирования и развертывания сети, включая обработку идентификаторов и адресов устройств, профилей использования сети и включение возможностей динамического управле-

ния. Управление сетями включает в себя контроль качества обслуживания, динамическое расширение сетей (для новых или обновленных устройств ИВ), обработку ошибок и контроль безопасности. Сети также обрабатывают динамическую и временную принадлежность мобильных устройств к сети при их входе или выходе из зоны действия сети.

7.4.11.2 Роль в системах ИВ

Некоторые сети управляются как часть системы ИВ, например, сети ближнего действия, соединяющие устройства ИВ. Другие сети, например, глобальные, не должны управляться как часть системы ИВ, поскольку они представляют собой сети общего назначения, часто эксплуатируемые другими организациями (например, сетями мобильной связи).

Управление сетями ИВ должно охватывать оба вида сетей и собирать их в единую систему, служащую целям системы ИВ. Когда системы ИВ используют сторонние сети связи общего назначения, по возможности могут быть использованы интерфейсы управления и эксплуатации сторонней сети.

7.4.11.3 Примеры

На заводе большинство датчиков и контроллеров на производственной линии используют локальную сеть для связи. Такие сети управляются и контролируются локально самим производством. Предприятие может также использовать облачные службы, расположенные удаленно. Связь между облачной службой и предприятием может быть организована на базе фиксированных или мобильных сетей. Такие сети управляются и контролируются оператором сети, а не производством. При этом производство может использовать интерфейсы от оператора сети для обеспечения защищенной и надежной связи между производством и облачным службой.

7.4.12 Способность работы в режиме реального времени

7.4.12.1 Описание

Способность работы в режиме реального времени — это свойство системы или режима работы, в которых вычисления проводятся за определенное время действия внешнего процесса с тем, чтобы результаты вычислений могли использоваться для контроля, мониторинга или своевременного реагирования на внешний процесс. Система способна выполнять действие/функцию или вызывать службу в течение определенного периода времени, тем самым поддерживая детерминированные операции.

7.4.12.2 Роль в системах ИВ

Для ИВ систем, работающих в режиме реального времени, необходимо, чтобы время реакции на события было предсказуемо и не изменялось при увеличении нагрузки.

7.4.12.3 Примеры

В системах управления процессом происходит непрерывный мониторинг датчиками таких параметров, как температура, расход, давление или состояние устройства, и проводится немедленное реагирование.

7.4.13 Самоописание

7.4.13.1 Определение

Самоописание — это процесс, когда компоненты системы ИВ перечисляют свои возможности для информирования других компонентов или систем ИВ для компоновки, функциональной совместимости и динамического обнаружения. Самоописание включает в себя спецификацию интерфейса, возможности компонента ИВ, список типов устройств для подключения к системе ИВ, список видов служб системы ИВ и текущее состояние системы ИВ. Сущности с самоописанием косвенно являются «четко определенными компонентами», согласно 7.3.11.

7.4.13.2 Роль в системах ИВ

Самоописание необходимо для компонуемости и функциональной совместимости систем и устройств ИВ. Самоописание является максимально эффективным в случаях, когда система ИВ взаимосвязана с другими системами ИВ, или в случаях, когда система ИВ расширяется за счет добавления новых устройств ИВ. Самоописание необходимо для мобильных устройств и для устройств в спящем режиме ввиду регулярного подключения к сетям и отключения от них.

7.4.13.3 Примеры

Примером самоописания является система, использующая Bluetooth в сетях ближнего действия, которая предоставляет имя устройства и список поддерживаемых служб при подключении.

Система транслирует свой статус и поддерживаемые службы и текущий уровень службы. Компонент принимает такую широковещательную информацию из множества сетей и систем и принимает решение о том, какая сеть обеспечит наилучшее соответствие требованию службы компонента. На основании решения компонент подключается к выбранной сети. Подобным образом работают сети Wi-Fi и Bluetooth.

7.4.14 Подписка на службу

7.4.14.1 Определение

Поставщики служб ИВ часто предоставляют подписку на службы ИВ пользователям ИВ. Поставщики служб ИВ предоставляют доступ к процессу подписки, с помощью которого пользователи ИВ могут подписаться на конкретную службу ИВ. Процесс подписки может включать в себя платежи и четкое указание предварительных условий для пользователя ИВ. Служба ИВ может включать в себя установку устройств ИВ, а также установку и настройку программных компонентов, предоставляемых или определяемых поставщиком служб ИВ. Подписка на службу и создание нового приложения ИВ может привести к установке новых требований безопасности к системе. Ответственность за выполнение требований безопасности лежит на подписчике, поскольку производитель системы ИВ не может предвидеть данный вариант использования.

В некоторых случаях пользователь ИВ может установить свою собственную службу ИВ, но в этом случае пользователь ИВ приобретает необходимое оборудование и программное обеспечение и несет последующие обязанности по эксплуатации и обслуживанию службы ИВ.

7.4.14.2 Роль в системах ИВ

Некоторые системы ИВ основаны на модели подписки, в которой пользователи ИВ оплачивают использование системы ИВ. В таких случаях поставщик служб ИВ должен установить четкие механизмы для установления и обслуживания подписок.

7.4.14.3 Примеры

Примером службы ИВ по подписке является предоставление персонального фитнес мониторинга. Пользователь ИВ приобретает носимое устройство ИВ, подключаемое к службе ИВ для отслеживания активности пользователя. Служба ИВ использует собранные данные для анализа и предоставляет отчет о деятельности и достижении целей пользователя.

8 Концептуальная модель ИВ

8.1 Основная задача

Концептуальная модель ИВ устанавливает общую структуру и определения для описания концепций, и взаимосвязей между сущностями в системах ИВ. Концептуальная модель должна быть общей, абстрактной и простой, для чего необходимо уточнить основные требования системы ИВ следующими вопросами:

- Какова общая модель сущностей ИВ и их взаимосвязей?
- Каковы ключевые понятия в типичной системе ИВ?
- Каковы взаимосвязи между сущностями, в частности, между цифровыми сущностями и их физическими сущностями?
- Кто и где является участником?
- Как вещи и службы взаимодействуют через сеть?

Концептуальная модель с учетом перечисленных пять вопросов определена в 8.2—8.3. Модель представлена с использованием унифицированного языка моделирования UML. Диаграммы в разделе 8 показывают два разных типа отношений между сущностями: обобщение и ассоциация. Более подробная информация приведена в приложении А.

8.2 Понятия концептуальной модели ИВ

8.2.1 Сущности и домены ИВ

8.2.1.1 Общие положения

Понятия сущностей и доменов ИВ представлены на рисунке 4.

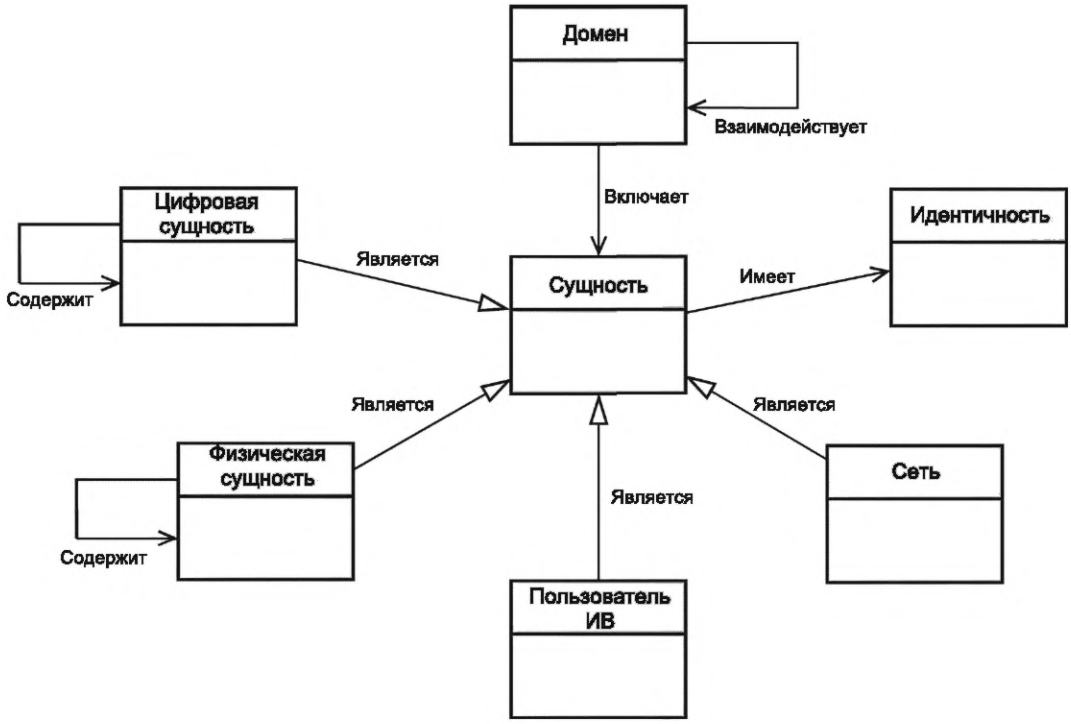

Рисунок 4 — Понятия сущностей и доменов концептуальной модели

Сущностью называется обособленно и независимо существующий объект, например человек, организация, устройство, подсистема или группа таких предметов. Все, что находится в системе ИВ, является своего рода сущностью. В концептуальной модели определяется четыре фундаментальных сущности: вещь (физическая сущность), пользователь (пользователь ИВ), ИТ-системы (цифровая сущность) и сети связи (сеть). Таблицы взаимосвязей сущностей для концептуальной модели приведены в приложении В.

Цифровая сущность — это один из вычислительных элементов и элементов данных системы ИВ, который включает в себя приложения, службы, виртуальные объекты, хранилища данных, устройства ИВ и шлюзы ИВ. Пользователь ИВ — это сущность, которая может быть или не быть человеком. Физическая сущность является дискретной, идентифицируемой и наблюдаемой. Сеть — сущность системы ИВ, через которую другие сущности взаимодействуют друг с другом. Сущности имеют идентичность через связанный идентификатор. Идентификаторы необходимы цифровым сущностям для взаимодействия с другими цифровыми сущностями через сеть. Существует множество форм идентификаторов, используемых в зависимости от свойств сущности.

При рассмотрении системы ИВ необходимо провести декомпозицию системы на части и сгруппировать сущности, которые служат общей цели, например определенной доменом. Сущности домена часто работают в подсистеме, связанной с этим доменом. Подсистемы и сущности домена могут взаимодействовать с подсистемами и сущностями другого домена. В таких случаях считают, что два домена взаимодействуют друг с другом. На рисунке 5 показано, как один домен А взаимодействует с другим доменом В. Один домен ИВ может взаимодействовать с несколькими доменами ИВ.



Рисунок 5 — Взаимодействия доменов концептуальной модели

8.2.1.2 Сущность

Сущность — это любой предмет (как материальный, так и нематериальный), который имеет отдельное и независимое существование. Каждая сущность имеет уникальную идентичность.

8.2.1.3 Домен

Домен является основной функциональной группой системы ИВ. Каждая сущность в системе ИВ включена (или содержится) в один или несколько доменов.

8.2.1.4 Цифровая сущность

Цифровая сущность — это вычислительный элемент или элемент данных системы ИВ, в том числе приложения, службы, виртуальные сущности, хранилища данных, устройства ИВ и шлюзы ИВ. Цифровая сущность — это специализированная сущность. Цифровая сущность может включать в себя другие такие сущности.

8.2.1.5 Физическая сущность

Физическая сущность — это дискретная, идентифицируемая и наблюдаемая часть физической среды. Физические сущности могут быть практически любым физическим объектом или средой: люди, животные, автомобили, магазины, логистические цепочки, компьютеры, электронные приборы, закрытые или открытые помещения и т. д. Физическая сущность — это специализированная сущность. Физическая сущность может содержать другие такие сущности.

8.2.1.6 Пользователь ИВ

Пользователь ИВ — это пользователь системы ИВ, который может быть или не быть человеком. Пользователь ИВ является частью системы ИВ. Пользователь ИВ — это специализированная сущность, представляющая пользователя или цифрового пользователя.

8.2.1.7 Сеть

Сеть — это инфраструктура, которая соединяет множество цифровых сущностей и обеспечивает обмен данными между ними. Сеть — это специализированная сущность.

8.2.2 Идентичность

8.2.2.1 Общие положения

На рисунке 6 показано понятие идентичности в отношении сущностей.

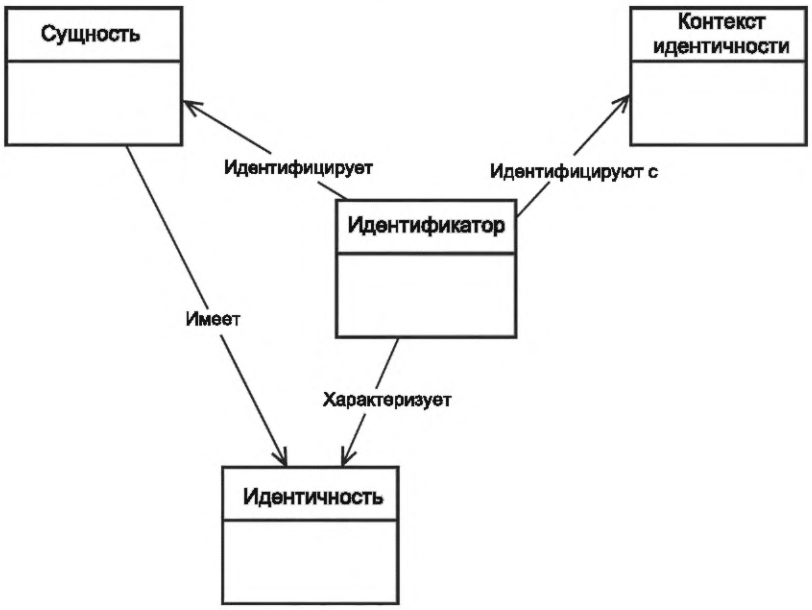

Рисунок 6 — Понятие идентичности в концептуальной модели

Многие сущности в ИВ, особенно физические сущности (вещи), имеют идентичность. Идентификатор — это набор атрибутов сущности, используемый для уникальной идентификации сущности в контексте. Сущность может иметь более одного идентификатора, но требуется как минимум один уникальный идентификатор в контексте идентичности, через который к ней можно получить доступ. Например, идентификационная информация из метки может использоваться в качестве идентификатора для идентификации физической сущности, к которой он присоединен.

8.2.2.2 Идентификатор

Идентификатор идентифицирует сущность. Идентификаторы характеризуют идентичность сущности. Сущность может иметь более одного идентификатора. Идентификаторы применяются в данном контексте идентичности.

8.2.3 Службы, сети, устройства и шлюзы ИВ

8.2.3.1 Общие положения

На рисунке 7 представлены взаимосвязи служб, устройств ИВ, шлюзов ИВ и соединяющих их сетей.

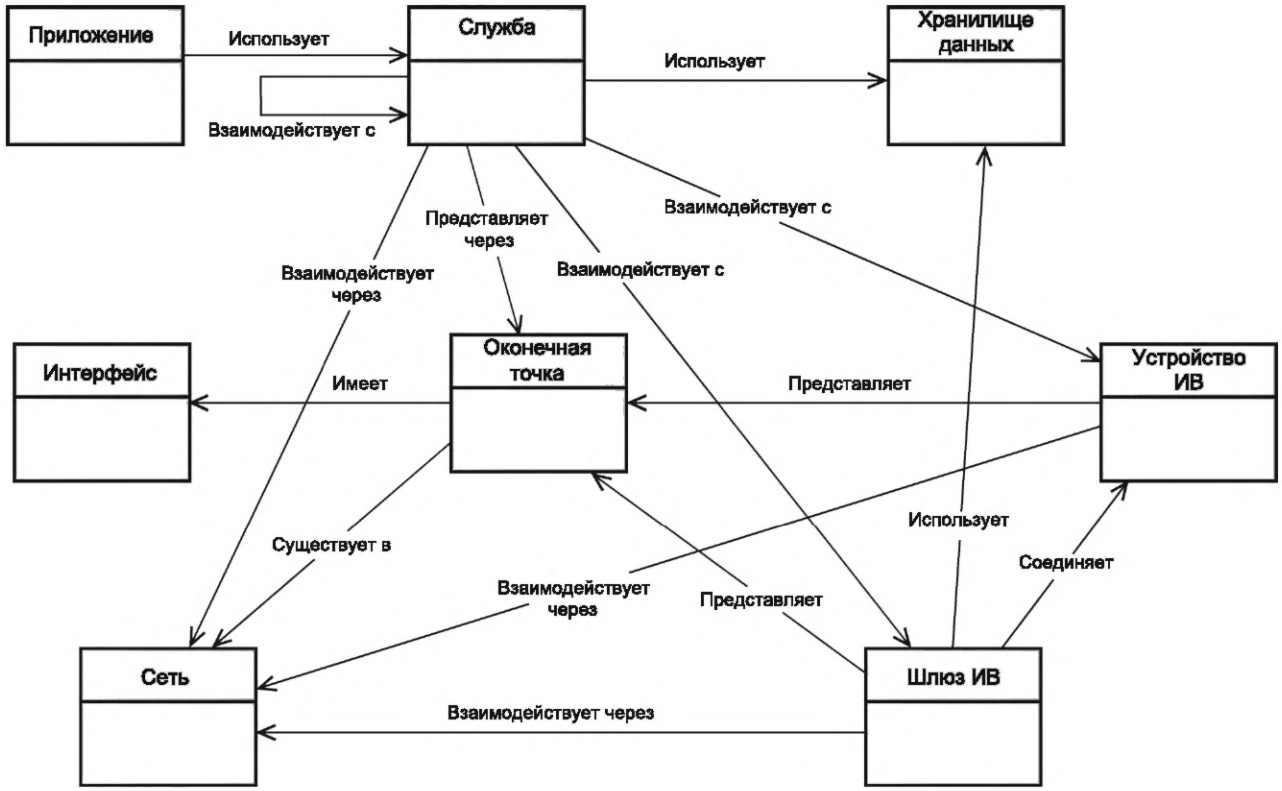

Рисунок 7 — Службы, сети, устройства и шлюзы ИВ

Служба является абстрактным понятием. Служба реализуется одним или несколькими компонентами. Может быть несколько реализаций одной и той же службы.

Сущности взаимодействуют через сети путем представления одной или нескольких оконечных точек в сети. Сеть соединяет оконечные точки. Служба представляет одну или несколько оконечных точек, с помощью которых может быть вызвана. Оконечная точка имеет один или несколько сетевых интерфейсов. Удаленные службы могут быть достигнуты оконечными точками через сетевые интерфейсы по сети связи. Оконечные точки существуют в одной или нескольких сетях.

Данные, связанные со службами, устройствами и шлюзами ИВ, могут храниться в хранилище данных, используемом одним или несколькими сущностями.

8.2.3.2 Оконечная точка

Оконечная точка либо реализует интерфейс, который может вызываться другими сущностями, либо соединяет сущность с интерфейсами других сущностей. Оконечная точка может содержать более одного интерфейса. Интерфейс — это набор операций и связанных параметров, которые могут использоваться одной цифровой сущностью для запроса действий у другой цифровой сущности.

8.2.3.3 Шлюз ИВ

Шлюзы ИВ образуют мост между различными сетями: между сетями ближнего действия, к которым подключены устройства ИВ, и сетями доступа (как правило, глобальными сетями), которые используют другие сущности в системе ИВ. Шлюзы ИВ могут использовать локальные хранилища данных. Шлюзы могут включать в себя функции безопасности для защиты обеих оконечных точек от сетевых атак или

для защиты транзитных сетей от вредоносных или поврежденных оконечных точек. Такие службы могут быть включены поставщиками служб либо в эксплуатационные, либо в дополнительные задачи.

8.2.3.4 Устройство ИВ

Устройство ИВ — это цифровая сущность, которая соединяет физические сущности реального мира с другими цифровыми сущностями системы ИВ через функции восприятия и приведения в действие. Устройство ИВ является как цифровой, так и физической сущностью, так как некоторые физические характеристики устройства ИВ влияют на его использование в системе ИВ, например местоположение, движение и ускорение устройства. Устройство ИВ взаимодействует с одной или несколькими сетями для связи с другими сущностями. Устройство ИВ должно иметь подключаемость сети и предоставлять одну или несколько оконечных точек, может содержать вычислительные возможности и опционально использовать локальные хранилища данных.

8.2.3.5 Служба

Служба — это набор отдельных возможностей, предоставляемых через определенный интерфейс. Служба может включать в себя другие службы. Служба обычно реализуется как программное обеспечение. Служба определяет сетевые интерфейсы и представляется оконечной точкой. Служба взаимодействует с другими сущностями через одну или несколько сетей. Служба взаимодействует с нулевым или большим количеством шлюзов ИВ, с нулевым или большим количеством устройств ИВ, с нулевым или большим количеством других служб. Службой может использоваться нуль или большее количество хранилищ данных.

8.2.3.6 Приложение

Приложение — это программное решение, предназначенные для содействия пользователям ИВ в осуществлении определенных задач или обработке конкретных видов задач ИТ посредством автоматизации процесса или функции бизнеса.

Приложение может использовать одну или несколько служб. Приложение может использоваться человеком ЧМИ или цифровым пользователем (через API).

8.2.3.7 Интерфейс

Интерфейс определяется как именованный набор операций, который характеризует поведение сущности. Интерфейс представляет собой набор операций и связанных параметров, которые могут использоваться одной цифровой сущностью для запроса действий от другой цифровой сущности.

8.2.3.8 Сеть

Сеть устанавливается путем подключения устройств и шлюза ИВ. Все соответствующие оконечные точки доступны через их интерфейсы.

8.2.3.9 Хранилище данных

Хранилища данных поддерживаются шлюзом ИВ и, опционально, устройствами ИВ. Хранилища данных содержат данные, относящиеся к системам ИВ. Данные могут быть получены непосредственно от устройств ИВ или от служб, обработавших данные от устройств ИВ.

8.2.4 Пользователь ИВ

8.2.4.1 Общие положения

На рисунке 8 представлены участники систем ИВ — пользователи ИВ.

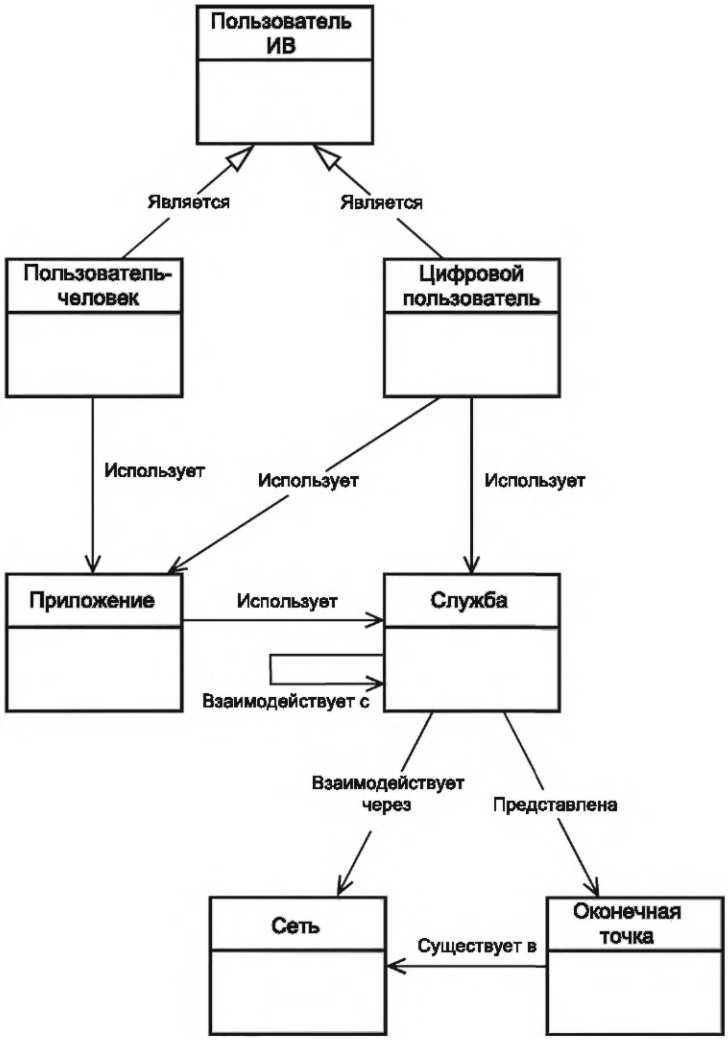

Рисунок 8 — Понятие пользователей ИВ

Пользователь ИВ может быть либо человеком (пользователь-человек), либо цифровым (цифровой пользователь). Цифровой пользователь включает в себя службы автоматизации, которые действуют от имени пользователя-человека, например при взаимодействии между компьютерами. Цифровой пользователь взаимодействует с одной или несколькими службами прямо или косвенно через оконечную точку службы. Пользователь-человек взаимодействует через одно или несколько приложений.

8.2.4.2 Пользователь-человек

Пользователь-человек — это человек, использующий систему ИВ. Пользователь-человек является специализированным пользователем ИВ. Пользователь-человек взаимодействует в сети через приложение.

8.2.4.3 Цифровой пользователь

Цифровой пользователь — это цифровая сущность, использующая систему ИВ. Цифровой пользователь является специализированным пользователем ИВ. Цифровой пользователь взаимодействует в сети с одной или несколькими службами, предлагаемыми системой ИВ.

8.2.4.4 Приложение

Приложение — это программная сущность или система, которая предоставляет набор функций, с помощью которых пользователь может выполнить задачу или достичь бизнес-цели. Приложение обычно использует службы. Функции приложения могут быть представлены как службы.

8.2.5 Виртуальная сущность, физическая сущность и устройство ИВ

8.2.5.1 Общие положения

На рисунке 9 представлены взаимосвязи между виртуальной сущностью, физической сущностью и устройством ИВ.

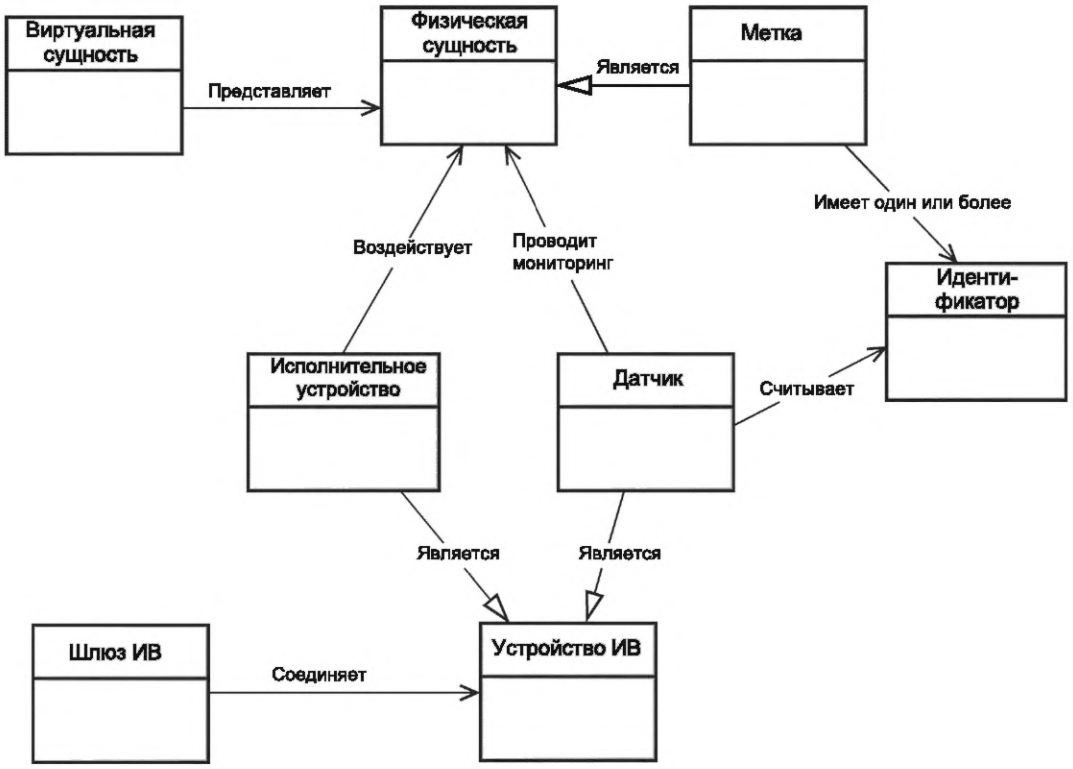

Рисунок 9 — Понятия виртуальной сущности, физической сущности и устройства ИВ

Исполнительные устройства и датчики — это устройства ИВ, которые имеют прямой или косвенный контакт с физической сущностью. Виртуальная сущность, метка, исполнительное устройство, датчик, идентификатор, шлюз ИВ и устройство ИВ являются цифровыми сущностями. Исполнительное устройство оперирует с полученной цифровой информацией для воздействия (изменения) на некоторые свойства физической сущности. Датчик воспринимает определенные характеристики физической сущности и преобразует их в цифровое представление, которое может передаваться. Физическая сущность может иметь одну или несколько прикрепленных меток, и датчики могут контролировать метку, а не непосредственно физическую сущность. Исполнительные устройства и датчики являются устройствами ИВ, которые количественно преобразуют изменения в одной физической величине в изменения в другой. Одно устройство ИВ может содержать несколько датчиков, например датчик местоположения и акселерометр в смартфоне.

Примером является смартфон с датчиком для определения температуры окружающей среды. Другим примером является случай, когда приложение Bluetooth на смартфоне соединяется с кондиционером для контроля температуры в помещении; в этом случае кондиционер является исполнительным устройством.

Следующий пример: смартфон имеет приложение для считывания штрих-кода. Приложение может иметь локально установленную базу данных (локальное хранилище данных) для поиска информации о штрих-коде сканируемого объекта или взаимодействовать с удаленной службой с размещением каталога через мобильную сеть. Штрих-код является одной из форм метки, прикрепленной к физической сущности.

8.2.5.2 Датчик

Датчик — это устройство, которое измеряет некоторые свойства физической сущности и выводит данные цифрового измерения. Цифровое измерение выходного сигнала датчика может значительно отличаться от исходной величины физической среды и может выводиться со значительной задержкой

по времени, в зависимости от обработки данных в устройстве. Примером может служить распознавание личности человека из устройства камеры наблюдения. Датчик является специализированным устройством ИВ *(см. 8.2.3.4)*. Датчик проводит мониторинг физической сущности.

8.2.5.3 Исполнительное устройство

Исполнительное устройство — это устройство, которое принимает цифровые входные данные и воздействует (изменяет) на одно или несколько свойств физической сущности на основе входных данных. Исполнительное устройство является специализированным устройством ИВ *(см. 8.2.3.4)*. Исполнительное устройство воздействует на физическую сущность.

8.2.5.4 Виртуальная сущность

Виртуальная сущность — это цифровое представление физической сущности в службе. Виртуальная сущность является цифровой сущностью. Виртуальная сущность может взаимодействовать через оконечную точку.

8.2.5.5 Метка

Метка — это физическая сущность, присоединенная к другой физической сущности для проведения ее идентификации и отслеживания. Метки могут иметь различные формы и быть пассивными или активными.

8.3 Высокоуровневое представление концептуальной модели

На рисунке 10 представлено высокоуровневое представление ключевых понятий концептуальной модели ИВ, их взаимосвязи и взаимодействия. Диаграмма не включает все понятия ИВ, которые представлены на рисунках ранее.

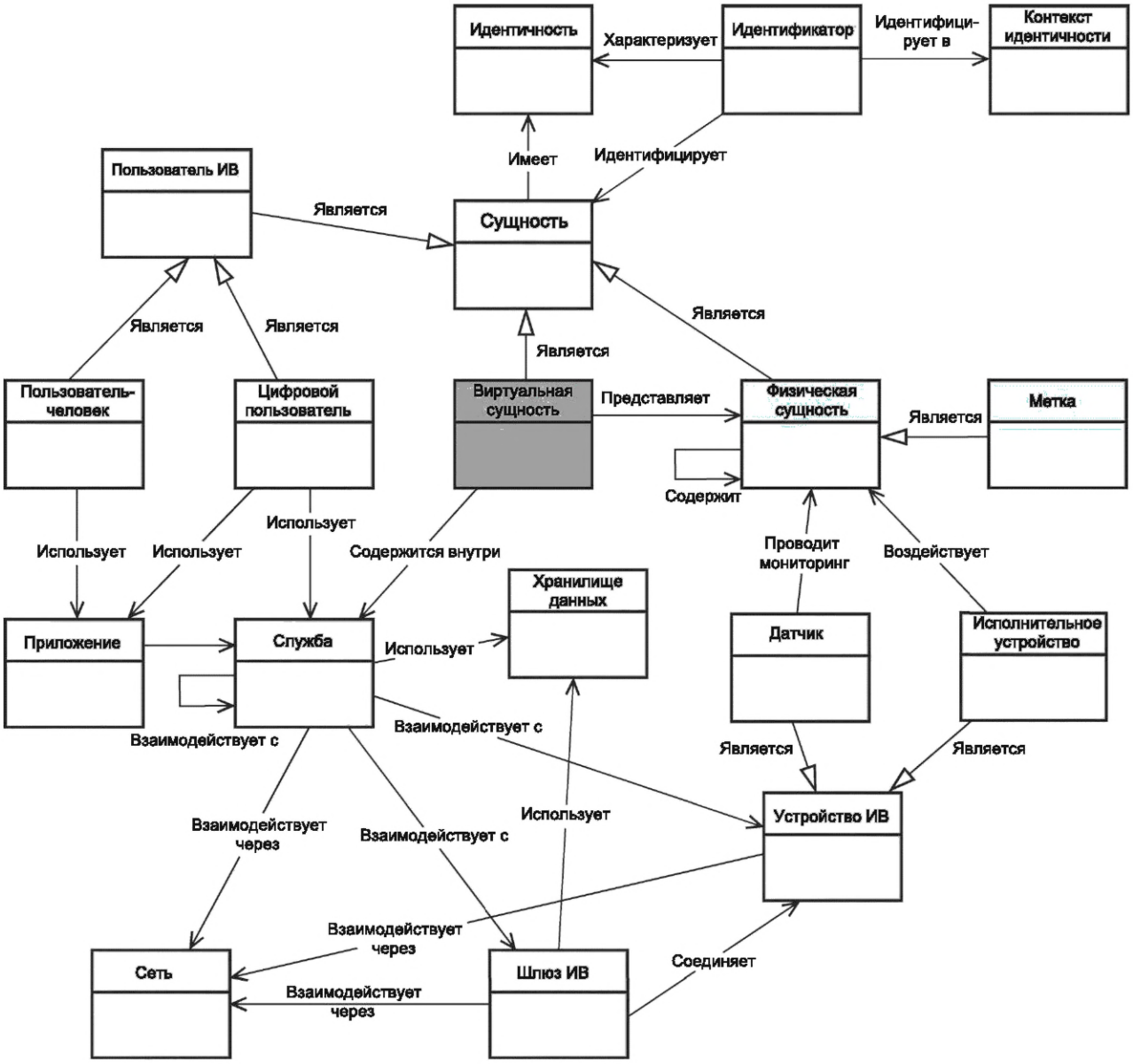

Рисунок 10 — Высокоуровневое представление концептуальной модели

Система ИВ включает в себя устройства, которые соединяют физические сущности в реальном мире с цифровыми сущностями путем взаимодействия через одну или несколько сетей. Сущности, определенные на рисунке 10 и в настоящем разделе, включены в систему ИВ. Пользователь ИВ может быть пользователем-человеком или цифровым пользователем, таким как роботы или службы автоматизации, которые действуют от имени пользователя-человека. Цифровой пользователь использует службы через сеть связи. Пользователь-человек взаимодействует с помощью приложений, которые являются специализированной формой служб. Некоторые приложения взаимодействуют с другими службами через сеть.

Физическая сущность — это реальный объект, который управляется исполнительным устройством или отслеживается датчиком. Физическая сущность может иметь прикрепленную метку, которая отслеживается датчиком вместо физической сущности. Виртуальная сущность представляет собой физическую сущность в мире ИТ. Виртуальная сущность — это цифровая сущность. Исполнительные устройства и датчики являются типами устройств ИВ. Устройства ИВ взаимодействуют через сеть и могут либо осуществлять связь на значительном расстоянии напрямую, либо связаны со шлюзом ИВ, осуществляющим связь на значительном расстоянии.

Хранилища данных содержат данные, относящиеся к системам ИВ. Данные могут быть получены непосредственно от устройств ИВ или от служб, обрабатывающих данные от устройств ИВ.

9 Типовая модель ИВ

9.1 *Общие положения*

Типовая модель ИВ является частью общей типовой архитектуры ИВ, представленной на рисунке 2.

Концептуальная модель и свойства системы ИВ определены в разделах 8 и 7 соответственно. Структура типовой модели ИВ и представления архитектуры определены в разделах 9 и 10. Взаимосвязи между концептуальной моделью, типовой моделью и типовой архитектурой представлены в приложении С. Типовая модель ИВ включает в себя типовую модель на основе сущностей и типовую модель на основе доменов.

9.2 Типовая модель ИВ

9.2.1 Типовая модель на основе сущностей

На рисунке 11 показана типовая модель на основе сущностей с указанием взаимодействий между основными сущностями.

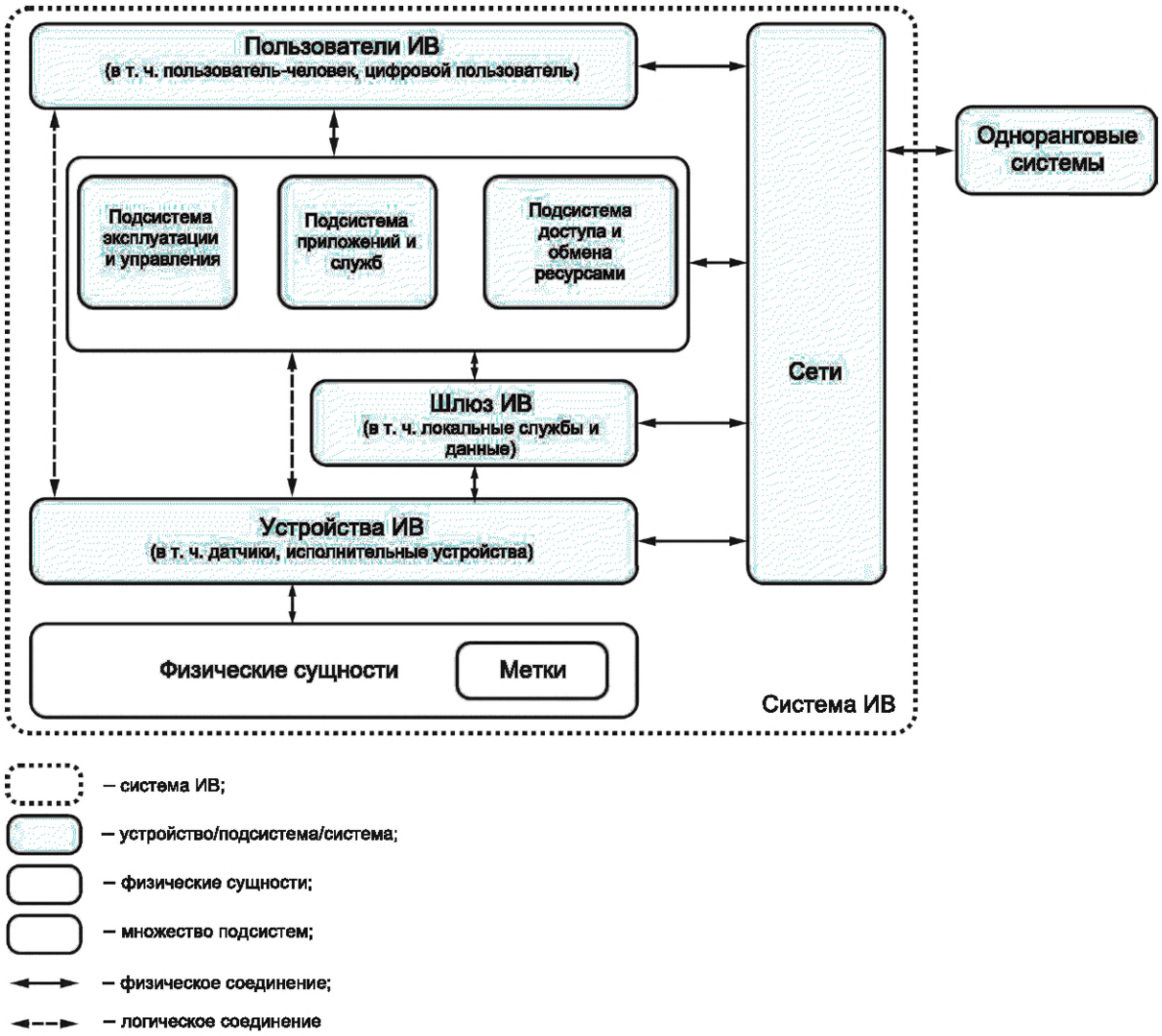

Рисунок 11 — Типовая модель на основе сущностей

Типовая модель на основе сущностей включает в себя:

а) физические сущности. Это предметы в реальном мире, которые воспринимаются устройствами ИВ, и на которых оказывается воздействие устройствами ИВ;

б) метки различных типов, которые могут быть прикреплены к физическим сущностям для облегчения их мониторинга и идентификации;

в) устройства ИВ, которые взаимодействуют с физическим миром через восприятие и приведение в действие. Устройства ИВ включают в себя:

1) датчики, которые измеряют свойство физической сущности и преобразуют измерение в цифровую информацию;

2) исполнительные устройства, которые воздействуют или изменяют некоторые свойства физических сущностей на основе цифровых инструкций;

г) сети, по которым устройства ИВ обмениваются данными. Многие устройства ИВ обмениваются данными по сетям с малым радиусом действия и специализированным сетям ближнего действия из-за ограничений по мощности и обработке. Другие устройства для коммуникации используют глобальные сети, например Интернет;

д) шлюзы ИВ, которые образуют канал между локальной сетью и глобальной сетью доступа. Шлюзы ИВ могут содержать другие сущности и предоставлять широкий спектр возможностей. Шлюз ИВ может содержать управляющего агента, который предоставляет функции удаленного управления. Шлюз ИВ может содержать хранилище данных для хранения данных от подключенных устройств ИВ, что позволит проводить локальную обработку (например, граничные или туманные вычисления) или функционировать в сетях с прерывистой связью. Шлюз ИВ может поддерживать одну или несколько служб аналитики, работающих с данными от устройств ИВ или с данными из хранилища данных устройства. Шлюз ИВ может содержать приложения, например приложение управления для управления приводами на основе входных данных от датчиков в случае, где требуется быстрая локальная обработка;

е) подсистемы приложений и служб, которые существуют в большинстве систем ИВ с хранилищами данных. Службы аналитики обрабатывают данные устройств и другие данные для получения информативных данных, например мониторинга производительности. Подсистема включает в себя управление процессами, которое контролирует процессы в системе ИВ. Подсистема может включать в себя приложения, которые представляют возможности системы ИВ. Могут быть представлены бизнес-службы, которые связаны с коммерческим использованием системы либо конечными пользователями, либо другими внешними одноранговыми системами. Приложения и службы взаимодействуют со шлюзами ИВ и устройствами ИВ через сеть доступа, а между собой — через сеть служб;

ж) подсистема эксплуатации и управления. Подсистема включает в себя хранилище данных реестра устройств и службу идентификации устройств, которая предоставляет функции поиска для приложений и служб. В состав подсистемы входит приложение для управления устройствами, которое обеспечивает мониторинг и возможности администрирования для устройств ИВ в системе. Подсистема включает в себя также систему поддержки эксплуатации, связанную с мониторингом и управлением всей системой ИВ, включая предоставление пользователям возможностей администрирования;

и) подсистема доступа и обмена ресурсами, которая предоставляет доступ к возможностям системы ИВ для пользователей и одноранговых систем и обеспечивает управляемые интерфейсы для служб, администрирования и бизнеса. Контроль доступа и предоставляемые возможности зависят от пользователя, поэтому требуется аутентификация и авторизация. Некоторые возможности могут быть предоставлены реализациями через интерфейсы облачных служб;

к) пользователи системы ИВ, которые могут включать в себя пользователя-человека и цифрового пользователя. Пользователь-человек обычно взаимодействует с системой ИВ с использованием какого-то пользовательского устройства, например, смартфона, персонального компьютера, планшета или специализированного устройства. Во всех случаях пользователю-человеку предлагается некоторая форма интерфейса приложения, предоставляемого базовым приложением, которое взаимодействует с остальной частью системы ИВ. Цифровые пользователи взаимодействуют с системами ИВ посредством API-служб, автономно управляемых подсистемой доступа и обмена ресурсами. И пользователь-человек, и цифровой пользователь взаимодействуют с остальной частью системы ИВ через пользовательскую сеть. В некоторых системах ИВ пользовательские устройства могут напрямую взаимодействовать с устройствами ИВ или шлюзами ИВ;

л) одноранговые системы, которыми могут быть системы ИВ или другие системы. Одноранговые системы становятся пользователями системы ИВ и/или предлагают системе ИВ службы. Взаимодействие с системой ИВ происходит через пользовательскую сеть, обычно через Интернет.

На рисунке 12 показаны наиболее распространенные сущности в системах ИВ.

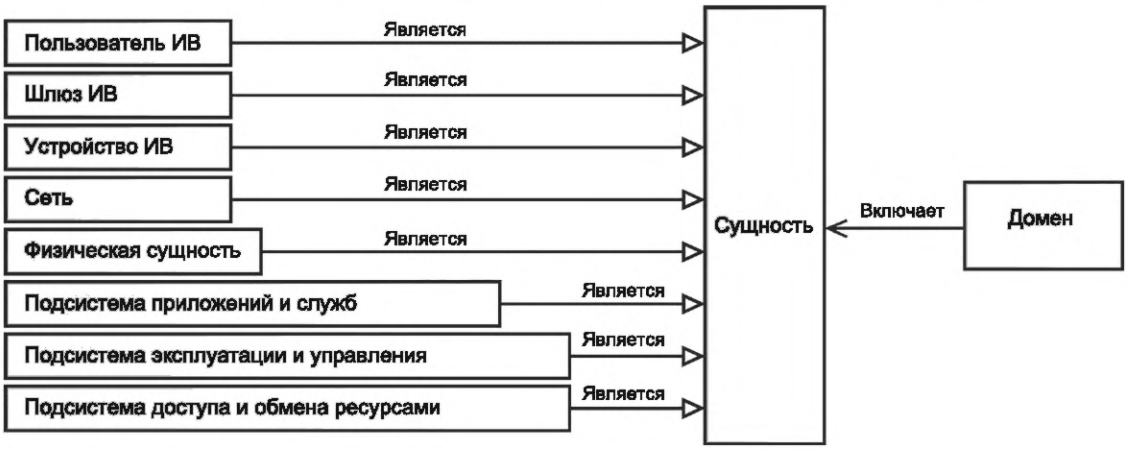

Рисунок 12 — Взаимосвязь домена с сущностью и сущностью в системах ИВ

9.2.2 Типовая модель на основе доменов

9.2.2.1 Общие положения

На рисунке 13 показана типовая модель на основе доменов. Домены разделяют задачи по логическому (иногда физическому) принципу. В основном, домены используются для группирования функций по областям ответственности. В типовой модели определены следующие домены: домен пользователей (UD), домен эксплуатации и управления (OMD), домен приложений и служб (ASD), домен доступа и обмена ресурсами (RAID), домен восприятия и контроля (SCD) и домен физических сущностей (PED). Каждый домен не пересекается с другими доменами. Взаимосвязь между типовой моделью на основе сущностей и типовой моделью на основе доменов приведена в 9.2.3. В разных представлениях каждый домен включает различные сущности. Сущности доменов в зависимости от представлений представлены в разделе 10.

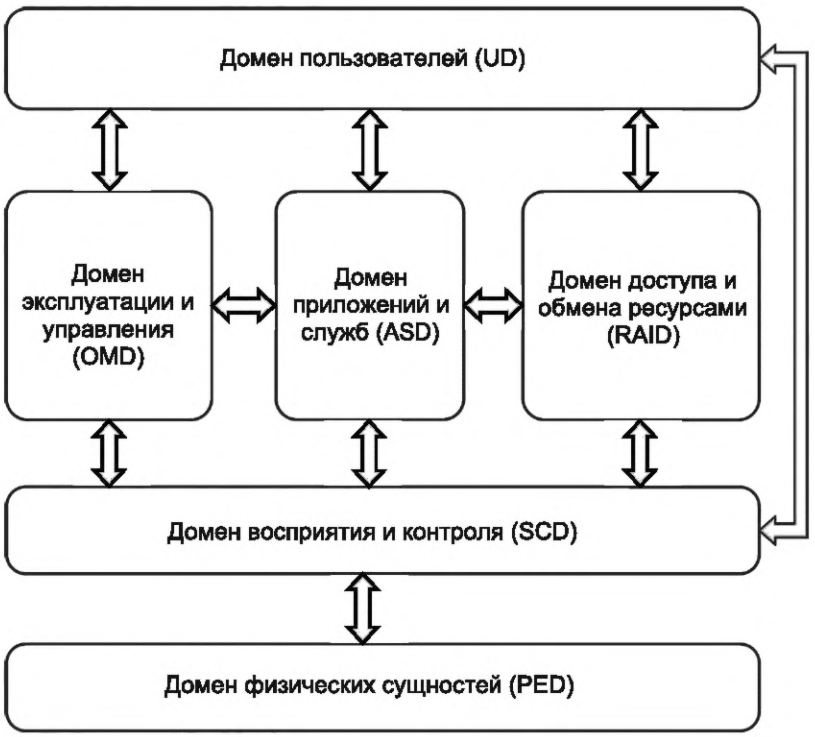

Рисунок 13 — Типовая модель на основе доменов

Взаимодействие доменов и сущностей происходит по множеству сетей, см. 10.4.

Сети связи не показаны в типовой модели на основе доменов, но являются важным компонентом любой системы ИВ. Сеть предоставляет путь для связи и обмена данными/информацией. Ключевая роль сетей заключается в обеспечении связи для обмена данными и взаимодействия между сущностями в доменах и между доменами.

9.2.2.2 Домен пользователей (UD)

Участниками UD являются пользователи. Пользователь может быть пользователем-человеком или цифровым пользователем. Пользователь-человек взаимодействует со службами через пользовательские устройства, через которые получают доступ к среде ИВ. Пользовательскими устройствами являются компьютеры, ноутбуки, смартфоны, планшеты и специализированные устройства для использования в интернете вещей, например, панели управления. Цифровые пользователи взаимодействуют со службами напрямую через интерфейсы.

9.2.2.3 Домен физических сущностей (PED)

PED включает в себя физические сущности в системе ИВ. PED является основной средой, в которой система ИВ отвечает за такие задачи или функции, как мониторинг, восприятие и контроль. Сущностями PED могут являться люди, но владелец PED не может быть сущностью PED.

9.2.2.4 Домен восприятия и контроля (SCD)

Устройства ИВ, а именно датчики, исполнительные устройства и сложные устройства ИВ, являются участниками SCD. SCD включает в себя датчики, которые проводят мониторинг свойств PED, и исполнительные устройства, которые могут воздействовать на PED. SCD является неотъемлемой частью системы ИВ, поскольку он соединяет виртуальную среду и реальный мир. SCD содержит другие сущности, включая шлюзы ИВ, локальные хранилища данных и локальные службы, в частности, службы управления.

9.2.2.5 Домен эксплуатации и управления (OMD)

Участниками OMD являются операторы и менеджеры системы ИВ, которые поддерживают общее состояние системы. OMD представляет собой функции, отвечающие за выделение ресурсов, управление, мониторинг и оптимизацию производительности системы в режиме реального времени. Как правило, OMD содержит OSS и BSS, с помощью которых происходит управление системой ИВ с точки зрения эксплуатации и с точки зрения бизнеса соответственно. OMD контролирует безопасный вывод системы ИВ из эксплуатации при возникновении необходимости.

9.2.2.6 Домен доступа и обмена ресурсами (RAID)

RAID предоставляет внешним сущностям механизмы доступа к возможностям системы ИВ. Основными классами внешних сущностей являются пользователи (взаимодействующие через пользовательские устройства) и одноранговые системы. Возможности системы ИВ предоставляются через один или несколько интерфейсов служб с контролируемым доступом. RAID содержит контролируемые оконечные точки, через которые предлагаются службы. Перечень доступных служб зависит от доступа для конкретной внешней сущности. Возможности RAID реализуются одним или несколькими другими доменами, в частности ASD и OMD.

9.2.2.7 Домен приложений и служб (ASD)

Участниками ASD являются поставщики приложений и служб, которые предлагают службы для пользователей ИВ в UD.

ASD содержит приложения и службы, предлагаемые поставщиками приложений и служб. Пользователи в UD взаимодействуют с приложениями и службами для выполнения своих запросов. Приложения и службы могут взаимодействовать с сущностями в SCD (в частности, с датчиками и исполнительными устройствами) для получения данных или исполнения действий в PED.

Приложения и службы могут предоставляться через облачные службы. Приложения и службы в ASD взаимодействуют с элементами в OMD, которые отвечают за управление ASD. Приложения и службы взаимодействуют с внешними сущностями через RAID, который может включать в себя внешние организации, такие как другие системы ИВ, системы иного типа, правительства, правоохранительные органы, финансовые учреждения, коммунальные службы.

9.2.3 Взаимосвязь между типовой моделью на основе сущностей и типовой моделью на основе доменов

Сопоставление типовой модели на основе сущностей и типовой модели на основе доменов приведено на рисунке 14.

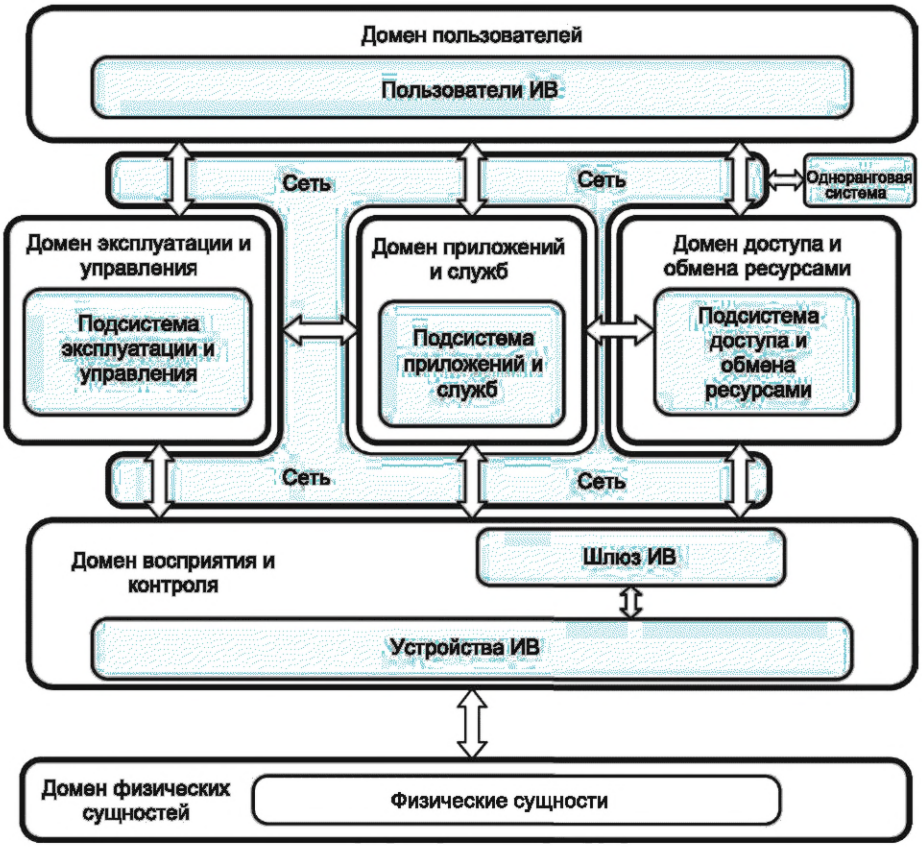

Рисунок 14 — Сопоставление типовой модели на основе сущностей и типовой модели на основе доменов

Пользователи ИВ относятся к домену пользователей. Подсистема приложений и служб относится к домену приложений и служб, подсистема эксплуатации и управления относится к домену эксплуатации и управления, подсистема доступа и обмена ресурсами относится к домену доступа и обмена ресурсами. Устройства ИВ и шлюз ИВ являются сущностями в домене восприятия и контроля. Физические сущности относятся к домену физических сущностей.

10 Представления типовой архитектуры ИВ

10.1 Общее описание

Типовая архитектура ИВ определяется четырьмя представлениями архитектуры:
- функциональное представление типовой архитектуры ИВ;
- представление развертывания типовой архитектуры ИВ;
- сетевое представление типовой архитектуры ИВ;
- преставление использования типовой архитектуры ИВ.

Типовая архитектура ИВ является базой, когда архитектура целевой системы используется для развертывания в конкретной системе. Примерами конкретных систем являются сельскохозяйственная система, система искусственного климата, система интеллектуальных сетей, умный дом/умное здание, умный город, умное предприятие и т. д.

10.2 Функциональное представление типовой архитектуры ИВ

10.2.1 Общие положения

Функциональное представление — это представление функциональных компонентов, необходимых для формирования системы ИВ, независимое от технологии. Функциональное представление определяет распределение и зависимости для поддержки деятельностей, определенных в представлении использования, и использует понятия функций домена и междоменных возможностей.

Каждый функциональный компонент представляет собой одну или несколько реализаций компонентов системы, установленных для формирования работающей системы. На рисунке 15 представлена декомпозиция функциональных компонентов типовой архитектуры ИВ. Функции домена и междоменные возможности являются необязательными для приложений ИВ. Функции домена являются общими и необязательными, и их необходимость определяется требованиями конкретного приложения.

10.2.2 Функции домена

10.2.2.1 Общие положения

Функции домена представлены на рисунке 15 в левой части рисунка.

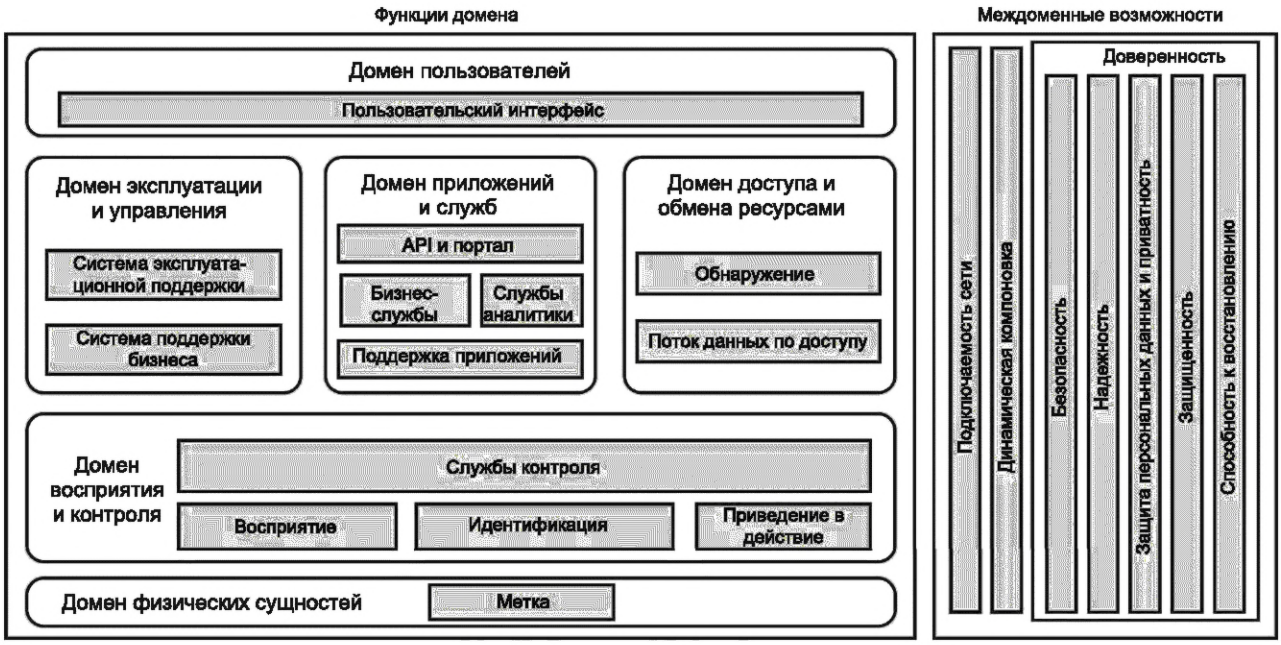

Рисунок 15 — Функциональное представление типовой модели

10.2.2.2 Домен восприятия и контроля (SCD)

SCD содержит набор общих функциональных компонентов, сложность реализации которых зависит от инфраструктуры систем ИВ.

а) восприятие — это функция считывания сенсорных данных с датчиков. Реализация функции соединяет аппаратное обеспечение, встроенное ПО, драйверы устройств и программные элементы;

б) приведение в действие — это функция записи данных и управляющих сигналов на исполнительное устройство для выполнения действия. Реализация функции соединяет аппаратное обеспечение, встроенное ПО, драйверы устройств и программные элементы. Функция является локальной в том смысле, что замыкает логический контур к датчикам и исполнительным устройствам. Реализация функции может физически размещаться совместно с другими центральными ресурсами при условии, что выполняются требования к способности к восстановлению и производительности;

в) службы контроля, которые необходимы для управления локальным состоянием в ASD, в частности, для выдачи команд исполнительным устройствам на основе входных данных от датчиков и других источников. Службы управления должны работать в режиме реального времени для того, чтобы обеспечивать надлежащее функционирование системы и безопасность эксплуатации при наличии динамических элементов в PED;

г) идентификация, которая обеспечивает идентифицируемость, обнаруживаемость и отслеживаемость сущностей в системе. Рекомендации к функции идентификации включают в себя следующее:

1) сущности должны идентифицироваться только в случае необходимости;

2) должна запрашиваться, собираться и обрабатываться только минимальная информация, необходимая для идентификации сущности;

3) необходимо различать ситуации идентификации устройства и идентификации индивида, связанного с устройством;

4) если идентифицирующая информация относится к физическому лицу, то она представляет собой персональные данные, и должны быть соблюдены соответствующие требования к защите и обработке персональных данных.

10.2.2.3 Домен приложений и служб (ASD)

Функции в ASD реализуют логику приложений и служб, которые предоставляют бизнес-функциональность для поставщиков служб в ASD. ASD содержит службы аналитики, службы когнитивных вычислений, службы потоковой передачи данных, службы управления процессами, службы визуализации, службы бизнес-правил, службы контроля и логику приложений. ASD также содержит хранилища данных различных типов, включая хранилище данных устройства, хранилище данных аналитики, хранилище архивных данных.

а) API и функции портала, которые обеспечивают контролируемый доступ к функциям системы ИВ цифровому пользователю и пользователю-человеку. Как правило, цифровой пользователь взаимодействует через API, пользователь-человек — через портал доступа. Если пользователи не являются частью доверенного домена системы ИВ, то доступ осуществляется через домен доступа и обмена ресурсами;

б) бизнес-службы, которые создают потоки бизнес-процессов и проводят оркестровку ресурсов для создания и управления службами;

в) службы аналитики, которые обрабатывают собранные данные (потоки сенсорных данных, другие контекстные данные и данные о внутреннем состоянии системы) для создания аналитических данных. Данные включают в себя события в реальном времени и/или архивные данные;

г) поддержка приложений, которая обеспечивает инфраструктуру для работы компонентов ASD и предоставляет инструменты, необходимые службе (и/или приложению) для ведения учета и выставления счетов.

10.2.2.4 Домен эксплуатации и управления (OMD)

OMD содержит два основных функциональных компонента, отвечающих за общее управление системой ИВ: OSS и BSS.

OSS проводит оперативное управление системой ИВ, включая выделение ресурсов, мониторинг и отчетность, управление политиками, автоматизацию служб, управление уровнем служб, ведение каталога служб, ведение реестров устройств и управление устройствами.

BSS отвечает за бизнес-аспекты системы ИВ, включая управление учетными записями, управление подписками, выставление счетов, ведение учетных записей и каталога продуктов.

10.2.2.5 Домен доступа к и обмена ресурсами (RAID)

10.2.2.5.1 Общие положения

RAID включает в себя необходимые и вспомогательные функции для доступа к ресурсам системы ИВ, как к службам, так и к данным, или для обмена ресурсами в системе ИВ. Доступ может быть в форме вызова службы или передачи данных. Участники доступа или обмена могут быть внутренними или внешними по отношению к системе ИВ (что меняется при интеграции систем ИВ в более крупную систему).

Ресурсы системы ИВ включают в себя любые возможности, предоставляемые системой ИВ:

а) службы различного характера (приложение, деятельности и управление);

б) данные и информация от датчиков или контроллеров, включая события и уведомления;

в) контекстные бизнес-данные;

г) полученные знания и информация, генерируемые приложениями и службами системы ИВ, например знания, созданные аналитическими процессами;

д) метаданные о системе ИВ и сущностях системы ИВ;

е) каталоги и репозитории для вышеперечисленного;

ж) возможности управления и ведения бизнеса.

Функции RAID позволяют обеспечить следующие аспекты обмена и доступа:

а) использование не только сетевых протоколов, но и протоколов передачи данных и сообщений, например, протоколов на основе REST и протоколов ИВ уровня сообщений или уровня данных;

б) контроль потоков данных и событий, обработка событий;

в) семантические описания, метаданные, систематизация, поддержка моделей данных и сопоставлений данных;

г) интерфейсы службы и управление ими;

д) обнаружение ресурсов и функции каталогов.

RAID поддерживает две основные функциональные группы, которые называют также функциональными компонентами:

- обнаружение;
- доступ к потоку данных.

10.2.2.5.2 Обнаружение

Функциональный компонент обнаружения обеспечивает доступ к ресурсам в системе ИВ для внешних и внутренних пользователей. Такими ресурсами являются приложения, службы и данные в ASD и могут быть возможности администрирования и бизнес-возможности, предлагаемые OMD. Функции компонента обнаружения включают в себя следующее:

а) идентификацию и адресацию оконечной точки службы;

б) интерфейсы ресурсов, в частности, для служб, и управление их жизненным циклом;

в) использование метаданных и управление ими;

г) доступ к каталогам и репозиториям и управление ими;

д) обнаружение ресурсов, размещение, поиск и запросы.

10.2.2.5.3 Доступ к потоку данных

Функциональный компонент доступа к потоку данных:

а) контролирует весь доступ к возможностям системы ИВ для внешних пользователей, включающих пользователей ИВ и одноранговые системы. Контроль доступа отвечает за все внешние оконечные точки системы ИВ и проводит необходимую аутентификацию и авторизацию для того, чтобы гарантировать использование возможностей системы ИВ только авторизованными пользователями. Контроль доступа включает в себя управление пользователями, определение и назначение ролей и групп;

б) содержит функции и процессы, связанные с передачей и подготовкой любой формы данных:

1) для периферийных данных от датчиков и контроллеров: предварительная обработка данных (очистка, уменьшение избыточности, консолидация, агрегация, преобразование, форматирование и сопоставление) и передача данных (потоковая передача данных и событий, управление потоком данных и маршрутизация);

2) для контроля: оркестрирование и поток управляющих операций и команд, отправка предупреждений и уведомлений, отправка исполняемого кода на периферию (например, туманные и граничные вычисления), отправка данных конфигурации на устройства.

10.2.2.6 Домен пользователей (UD)

Функциональные компоненты домена пользователей предоставляют пользователю доступ к возможностям системы ИВ.

Пользователь-человек взаимодействует с возможностями системы ИВ через приложение с пользовательскими интерфейсами. Цифровой пользователь взаимодействует через API, в которых возможности системы ИВ предоставляются по сети.

Домен пользователей содержит пользовательские устройства, которые поддерживают приложения для пользователей-людей.

10.2.2.7 Домен физических сущностей (PED)

PED содержит физические сущности, которые относятся к системе ИВ.

Функциональные компоненты данного домена являются метками, которые могут быть прикреплены к физическим сущностям.

10.2.3 Междоменные возможности

10.2.3.1 Общие положения

На рисунке 15 показан набор междоменных функциональных компонентов. Основной междоменной функцией является подключаемость сети. На рисунке 15 показан функциональный аспект доверенности (защищенность, приватность и защита персональных данных, безопасность, надежность и способность к восстановлению), хотя характеристики доверенности определяются в более широком смысле как характеристики системы (см. раздел 7) и имеют влияние на все другие представления типовой архитектуры ИВ.

10.2.3.2 Подключаемость сети

Сети и протоколы подключают сущности и подсистемы из более чем одного функционального домена, таким образом соединяя между собой домены. Сети в системе ИВ включают в себя:

- сеть ближнего действия, которая обеспечивает передачу данных от активов или устройств на периферии, к сущностям, например, шлюзам, которые обрабатывают данные для дальнейшей передачи к сущностям из других доменов или для управляющих действий, например, в граничных или туманных вычислениях. Сеть ближнего действия позволяет управлять активами через исполнительные

устройства или контроллеры. Сеть ближнего действия ограничивается SCD, но в некоторых случаях сеть ближнего действия является и сетью доступа;

- сеть доступа, которая позволяет передавать периферийные данные (из SCD) в логику приложения (из ASD) или эксплуатационную логику (из OMD). Сеть доступа позволяет передавать средства управления сущностям SCD от сущностей и подсистем ASD и OMD. Сеть доступа поддерживает функции управления и связи более высокого уровня (из RAID);

- сеть служб, которая соединяет приложения и службы в ASD, RAID и OMD. Сети служб позволяют разворачивать приложения ИВ на основе служб, например, с использованием микрослужб и других служб с возможностью совместной работы;

- пользовательская сеть, которая предоставляет доступ к функциям ASD и OMD пользователям-людям и цифровым пользователям. Пользовательская сеть обеспечивает более высокий уровень интеграции между различными системами ИВ, а также с системами, не относящимися к ИВ, благодаря поддержке взаимодействия сущностей RAID с пользователем.

10.2.3.3 Доверенность

Характеристики достоверности (см. раздел 7) (безопасность, приватность и защита персональных данных, защищенность, способность к восстановлению и надежность) имеют в основе междоменные функции:

а) функции безопасности в системе ИВ обеспечивают общую безопасность системы ИВ, а также безопасность конкретных компонентов системы;

б) функция приватности и защиты персональных данных распространяется на все элементы системы ИВ, независимо от того, где создаются, хранятся и обрабатываются персональные данные. Функция защиты персональных данных отслеживает наличие и местонахождение персональных данных. Функция защиты персональных данных применяет комплекс мер для обеспечения надлежащей защиты персональных данных, включая шифрование хранимых и передаваемых персональных данных, анонимизацию, агрегирование и контроль доступа к персональным данным только для авторизованных пользователей;

в) функции защищенности в системе ИВ обеспечивают конфиденциальность, доступность, целостность, подлинность информации. Типовая архитектура ИВ объединяет политики защищенности для компонентов ИВ как ключевую часть проектирования системы. Например, управление активами в SCD обеспечивает эксплуатационное управление, в том числе конфигурацией системы, политикой, обновлениями программного обеспечения и встроенного программного обеспечения и другими элементами управления жизненным циклом;

г) функции способности к восстановлению позволяют системе ИВ оперативно восстанавливать рабочее состояние после инцидента. Функции способности к восстановлению тесно связаны с автономными вычислительными возможностями самовосстановления, самоконфигурирования, самоорганизации и самозащиты;

д) функции надежности гарантируют, что система ИВ или ее компоненты выполняют требуемые функции в указанных условиях в течение определенного периода времени.

10.2.3.4 Динамическая компоновка

Функции динамической компоновки обеспечивают интеграцию и развитие системы ИВ благодаря быстрой интеграции новых сущностей в систему, доступности исчерпывающих метаданных и наличию гибких интерфейсов.

10.3 Представление развертывания системы типовой архитектуры ИВ

10.3.1 Общие положения

Представление развертывания системы определяет общие компоненты для формирования системы ИВ, в том числе устройства, подсистемы и сети. В то время как функциональное представление определяет систему ИВ через ее функциональные компоненты, представление развертывания системы представляет ее через ее компоненты реализации. Представление развертывания системы определяет:

а) ключевые физические компоненты системы ИВ (например, подсистемы, устройства, сети);

б) общую архитектуру реализации системы ИВ, включая структуру системы ИВ, распределение компонентов и топологию взаимосвязанности компонентов;

в) техническое описание компонентов, включая режим работы и другие свойства.

На рисунке 16 показано представление развертывания системы типовой архитектуры ИВ с сущностями каждого домена и соединениями между ними. Сущности в каждом домене являются общими и необязательными и определяются требованиями конкретных приложений.

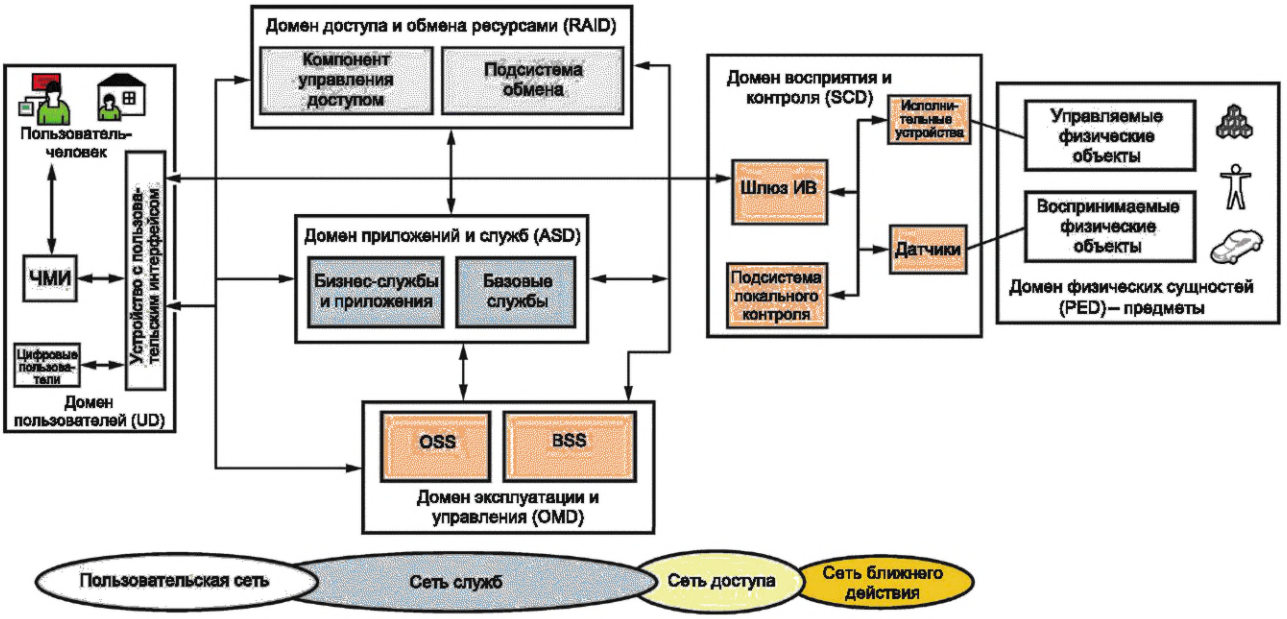

Рисунок 16 — Представление развертывания типовой архитектуры ИВ

Соединение физических компонентов в шести доменах системы ИВ проводится по четырем видам сетей: сеть ближнего действия, сеть доступа, сеть служб и пользовательская сеть *(см. 10.4)*.

10.3.2 Системы/подсистемы в домене физических сущностей (PED)

PED включает в себя воспринимаемые физические объекты и управляемые физические объекты, которые связаны с приложениями ИВ и представляют интерес для пользователей. Воспринимаемый физический объект — это физический объект, информация от которого поступает на датчики. Управляемый физический объект — это физический объект, на который оказывается воздействие исполнительными устройствами.

10.3.3 Системы/подсистемы в домене восприятия и контроля (SCD)

Сущности в SCD включают в себя датчики, исполнительные устройства и шлюзы ИВ. Датчики считывают свойства физических сущностей, а исполнительные устройства изменяют свойства физических сущностей.

Датчики получают информацию о свойстве физической сущности (например, физическом, химическом, биологическом). Исполнительные устройства изменяют свойства сущностей. Датчики и исполнительные устройства могут взаимодействовать с физическими сущностями независимо или совместно.

Шлюзы ИВ — это устройства, которые связывают SCD с другими доменами. Шлюзы ИВ обеспечивают такие функции, как преобразование протоколов, сопоставление адресов, обработка данных, объединение информации, сертификация и управление оборудованием. Шлюзы ИВ могут быть независимым оборудованием или интегрированы с другими датчиками и исполнительными устройствами. Шлюз ИВ также может выполнять функции защищенности для устройств ИВ, подключаемых к сетям.

SCD может содержать системы локального управления, которые используются для запуска служб управления, т. е. компонентов для локального управления возможностями шлюза ИВ.

10.3.4 Системы/подсистемы в домене приложений и служб (ASD)

Целью подсистемы ASD является размещение основных функций, служб и приложений, которые предоставляют функциональные возможности системы ИВ пользователям (людям и/или цифровым пользователям).

Подсистема ASD предоставляет базовые службы, включая вычислительные, такие как доступ к данным, обработка данных, объединение данных, хранение данных, установка идентификаторов, служба географической информации и управление пользователями, а также управление запасами.

В подсистеме ASD размещаются бизнес-службы и приложения, созданные на базовых службах, поскольку возможность размещения приложений является одной из служб, предоставляемых системами ИВ.

10.3.5 Системы/подсистемы в домене эксплуатации и управления (OMD)

Подсистема OMD содержит компоненты управления устройствами ИВ и контроля эксплуатации системы ИВ для обеспечения того, что оборудование и системы работают безопасно и надежно. Подсистема проводит мониторинг системы на предмет того, что соответствующие законы и правила не нарушены.

OMD содержит OSS и BSS.

OSS отвечает за общую работу системы ИВ и включает в себя возможности мониторинга и управления всеми сущностями системы ИВ в течение их жизненного цикла. OSS включает в себя системы проверки соответствия, которые проверяют систему ИВ на соответствие законам, нормативным актам и политикам организации.

BSS отвечает за реализацию бизнес-аспектов системы ИВ. Бизнес-функции включают CRM, управление подписками, выставление счетов и обработку платежей.

10.3.6 Системы/подсистемы в домене пользователей (UD)

UD включает пользователей-людей и цифровых пользователей. Цифровые пользователи — это устройства определенного типа, которые напрямую взаимодействуют с другими сущностями в системе ИВ через сетевые интерфейсы или API. Пользователь-человек взаимодействуют с системой ИВ с помощью пользовательского устройства с ЧМИ.

Подсистема ЧМИ включает в себя устройства и вспомогательное программное обеспечение для взаимодействия пользователя-человека с системой ИВ. В зависимости от роли пользователя, для наблюдения и управления в подсистеме представлены различные аспекты системы.

10.3.7 Системы/подсистемы в домене доступа и обмена ресурсами (RAID)

RAID включает компонент управления доступом и подсистему обмена.

Компонент управления доступом аутентифицирует и авторизует внешних пользователей системы ИВ, запрашивающих доступ к возможностям системы ИВ. Когда система ИВ должна использовать информацию и возможности, предоставляемые партнерской системой ИВ, то используется обратное управление доступом.

Подсистема обмена обеспечивает предоставление возможностей в системе ИВ, например приложения, данные и службы в ASD и возможности администрирования и бизнес-возможности в OMD. Возможности в OMD позволяют автоматизировать установление доверительных отношений по данным авторизации.

10.4 Сетевое представление типовой архитектуры ИВ

10.4.1 Сети связи

10.4.1.1 Общие положения

Сетевое представление типовой архитектуры ИВ определяет основные сети связи в системах ИВ и подключаемые сущности. На рисунке 17 показаны четыре вида сетей связи.

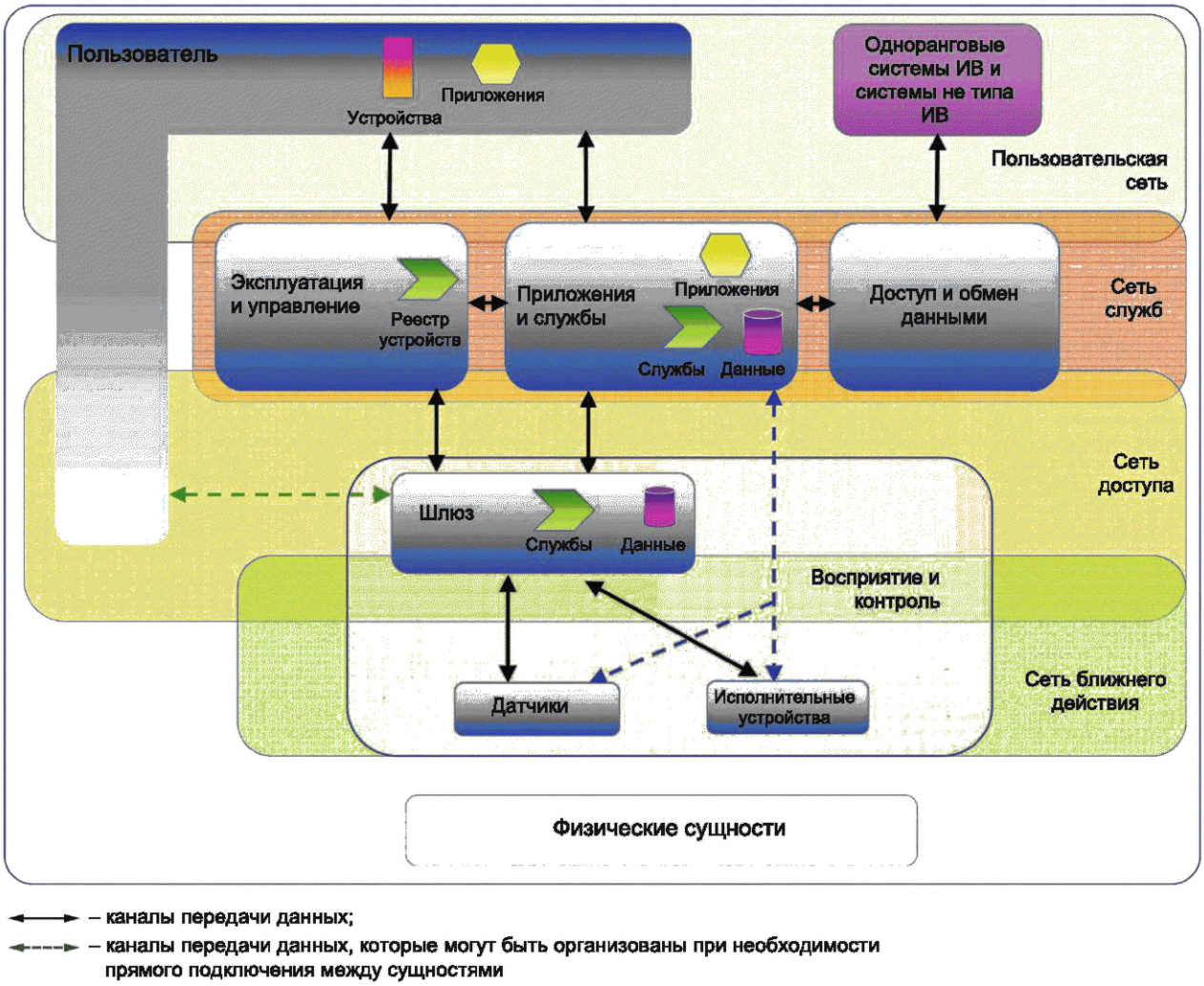

Рисунок 17 — Сетевое представление типовой архитектуры ИВ

Взаимосвязанные сети обеспечивают подключаемость сети, в том числе каналы передачи данных. Каналами передачи данных могут быть двухточечные соединения внутри или между системами ИВ, внутри или между доменами, а также с другими системами и организациями. Подключенные сети должны управлять подключаемостью от одной сети до другой. Ключевая роль сетей заключается в поддержке и обеспечении деятельностей и взаимодействий для коммуникаций и обмена данными. Типы деятельностей и взаимодействий между двумя сущностями, между двумя доменами или между двумя системами ИВ определяют их взаимосвязи между сущностями, доменами и системами ИВ соответственно. В зависимости от инфраструктуры систем ИВ междоменными сетями связи могут быть локальная сеть, Интернет, интрасеть, магистральная сеть предприятия, межкорпоративная сеть (Business-to-business, B2B) или глобальная сеть.

10.4.1.2 Сеть ближнего действия

Сеть ближнего действия существует в домене восприятия и контроля. Основная задача сети — подключение датчиков и исполнительных устройств к системе ИВ. Сети ближнего действия, как правило, являются локальными и имеют ограниченный радиус действия, поскольку датчики и исполнительные устройства имеют низкое энергопотребление или находятся в местах, которые затрудняют или делают невозможным использование глобальной сети (например, Интернет).

Сети ближнего действия используют общие протоколы или специализированные протоколы.

Сети ближнего действия могут включать в себя трансляцию адресов для преобразования между локальными схемами адресации и схемами адресации в сетях доступа.

10.4.1.3 Сеть доступа

Как правило, сети доступа являются глобальными сетями, соединяющими устройства в SCD с доменами ASD и OMD. Сети доступа подключаются к шлюзам, но датчики и исполнительные устройства могут подключаться непосредственно к сетям доступа в ситуации ограничения подключений (пунктирные линии на рисунке 17).

В сетях доступа используются проводные соединения (широкополосные сети, ADSL, оптоволоконные сети) и беспроводные соединения (беспроводные локальные сети, мобильные (сотовые) сети, глобальные сети с низким энергопотреблением, спутниковые каналы для удаленных местоположений).

Сети доступа обычно используют IP. Сети доступа могут включать использование реестра устройств, в котором хранятся данные об устройствах ИВ и способы связи с ними.

10.4.1.4 Сеть служб

Сеть служб соединяет приложения и службы в ASD, RAID и OMD, которые обычно являются проводными сетями с центрами обработки данных и используют протоколы на основе IP. Сеть служб может включать в себя как элементы Интернета, так и элементы интрасети (частной сети). Интрасеть используются там, где элементы других доменов существуют в одном центре обработки данных. Если коммуникации охватывают несколько центров обработки данных, то используются различные сетевые технологии, в том числе выделенные соединения и интернет-соединения.

10.4.1.5 Пользовательская сеть

Пользовательская сеть соединяет домен пользователей с ASD и OMD, а также соединяет RAID и одноранговые системы ИВ или системы, не относящиеся к ИВ. Сеть обычно основана на общедоступных элементах Интернета и использует IP. Пользовательские сети используют любую проводную или беспроводную технологию, примененную для передачи интернет-трафика.

10.4.2 Реализация сетей связи

Каждая из сетей связи реализуется с помощью сетевых технологий в зависимости от конкретных характеристик и требований системы ИВ. Реализации системы ИВ могут использовать несколько экземпляров каждого типа сетей. Функциональная совместимость между системами ИВ определяется тем, насколько корректно передаются данные/информация из одного типа сети в другой тип сети. Шлюзы ИВ являются компонентом сети связи для соединения неоднородных сетей связи. Функциональная совместимость приложений ИВ также требует адаптации новых сетей связи ИВ к устаревшим сетям связи.

Системы ИВ используют различные топологии сети для поддержки функциональности и возможностей ИВ. Распространенными топологиями сети являются точка—точка (постоянная или коммутируемая), шина (линейная или распределенная), звезда (расширенная или распределенная), кольцо, ячеистая (полностью подключенная или частично подключенная), одноранговая и гибридная (комбинация двух или более топологий).

На рисунке 17 показан домен пользователей, охватывающий пользовательскую сеть и сеть доступа. Примером является подключение пользовательских устройств и их приложений непосредственно к SCD, например, когда пользовательское устройство представляет собой смартфон с датчиками.

10.5 Представление использования типовой архитектуры ИВ

10.5.1 Общее описание

Представление использования определяет, каким образом система ИВ разрабатывается, тестируется, эксплуатируется и используется с точки зрения пользователя. В представлении рассматриваются деятельности, роли и подроли, службы и сквозные аспекты.

10.5.2 Роли, подроли и деятельности

10.5.2.1 Общие положения

Деятельности, связанные с ИВ, включают в себя три группы пользователей:

а) поставщик служб ИВ;

б) разработчик служб ИВ;

в) пользователь ИВ.

На рисунке 18 представлены три группы пользователей (роли) и их подроли. Синие стрелки показывают взаимодействие при использовании. Определение ролей и подролей представлено в 10.5.2.2, 10.5.2.3 и 10.5.2.4.

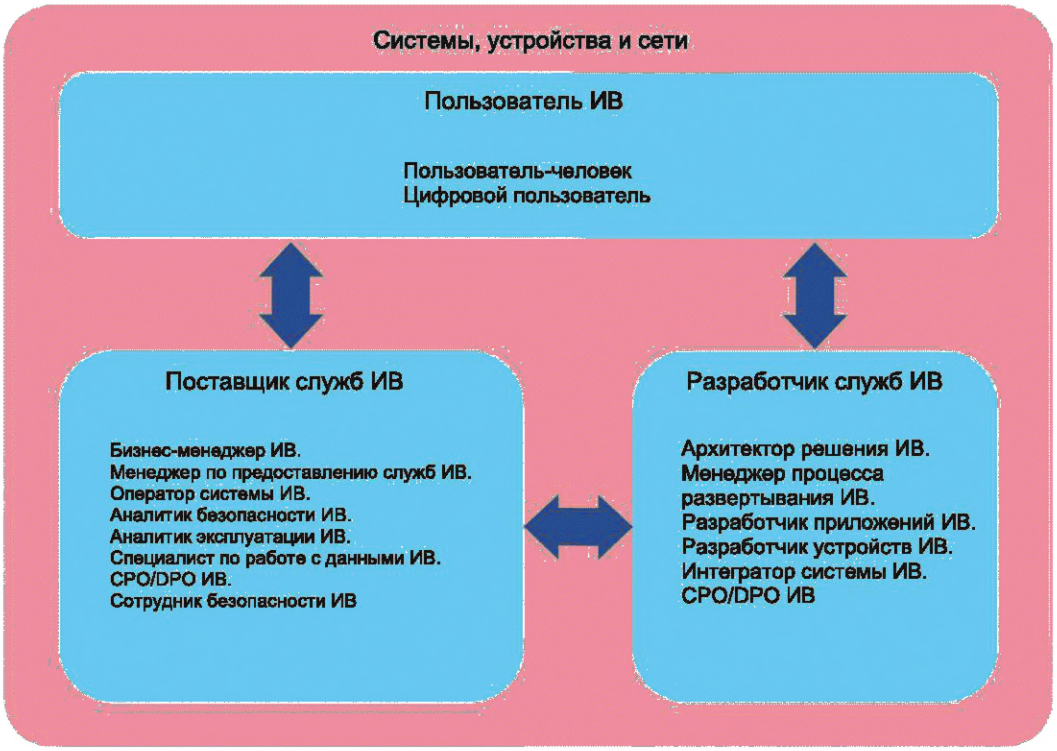

Рисунок 18 — Роли при использовании системы ИВ

10.5.2.2 Поставщик служб ИВ

Роль поставщика служб заключается в управлении и эксплуатации служб ИВ. Поставщики служб ИВ могут обеспечивать подключаемость сети. Должна быть рассмотрена и обеспечена защищенность подключаемости сети. Для облачных служб ИВ в зависимости от типа службы, предлагаемой в центре обработки данных (SaaS, PaaS, IaaS), на разных уровнях стека от аппаратного обеспечения до прикладного уровня должны проводиться управление защищенностью, мультиаренда, защита арендатора и разделение. Поставщик служб ИВ включает в себя следующие подроли.

- бизнес-менеджер ИВ ведет бизнес с существующими и новыми продуктами. В задачи бизнес-менеджера входит понимание, как могут быть использованы данные и подключаемость устройств для создания новых доходов. Бизнес-менеджер изучает отраслевой контент на веб-сайтах компаний и принимает решения по предлагаемым предложениям архитекторов;
- менеджер по предоставлению служб ИВ отвечает за соглашение об уровне обслуживания между клиентом и LOB. Совместно с командой инженеров по обслуживанию они используют платформу с поддержкой ИВ и отраслевые бизнес-приложения для планирования, установки, мониторинга и обслуживания оборудования. Данная роль обеспечивает, что общее качество предоставления служб находится в пределах параметров соглашения об уровне обслуживания;
- оператор системы ИВ осуществляет ежедневное обслуживание системы путем регистрации новых пользователей и проверки того, что новые типы устройств и устройства зарегистрированы, работают корректно и соответствуют текущей версии прошивки устройств;
- аналитик безопасности ИВ снижает риски безопасности путем создания алгоритмов по обнаружению угроз и предотвращению нарушений. Аналитик безопасности создает автоматические функции, которые влияют на ненадлежащие действия устройств и пользователей ИВ, а также обеспечивает соответствие посредством аудита;
- аналитик эксплуатации ИВ отвечает за доступность определенных активов в линейке продуктов LOB, для чего использует возможности анализа больших данных в платформе ИВ и алгоритмические расширения служб специалиста по работе с данными;
- специалист по работе с данными ИВ компетентен в вопросах отраслевых данных, поступающих с устройств, и алгоритмов эффективного анализа данных. Специалист по работе с данными ИВ

реализует прогрессивные алгоритмы в качестве служб, которые используются аналитиками LOB и отраслевыми приложениями LOB;

- руководитель службы по вопросам приватности/специалист по защите данных ИВ имеет следующие должностные обязанности (список является неполным): консультирование организации по обязательствам согласно законодательству о приватности/защите данных, контроль за реализацией и применением политики и обучения в области защиты персональных данных в организации, мониторинг нарушений в отношении персональных данных и реагирование на запросы регулирующих органов;

- менеджер по защищенности сети и инфраструктуры ИВ отвечает за обеспечение защищенности эксплуатационной инфраструктуры и подключаемости сетей, что включает (список является неполным): обеспечение доступности, целостности и конфиденциальности (где это применимо) сетей, инфраструктуры системы и управления безопасностью. В сферу ответственности менеджера входят датчики и физическое оборудование, в том числе оборудование для центров обработки данных, общедоступные облачные службы, инфраструктура связи, доступ арендаторов, аспекты защищенности арендаторов и т. д.;

- аналитик/инженер по вопросам приватности ИВ рассматривает общие аспекты приватности системы ИВ, включая пользователей/потребителей служб ИВ, с целью защиты от утечки приватности и соответствия нормативным требованиям. Аналитик/ инженер по вопросам приватности ИВ отвечает за проектирование и оценку системы с точки зрения защиты приватности и использует существующие методы защищенности и архитектуры безопасности для оценки приватности служб ИВ;

- специалист по безопасности ИВ отвечает за все аспекты безопасности системы, в том числе различных компонентов и подсистем. Это включает (список является неполным): обеспечение безопасности всех пользователей и операторов, документирование политик и процедур безопасности, выполнение проверок безопасности, оценку и реализацию соответствия нормативным требованиям безопасности и проведение расследований инцидентов безопасности.

На рисунке 19 показаны деятельности подролей поставщика служб ИВ.

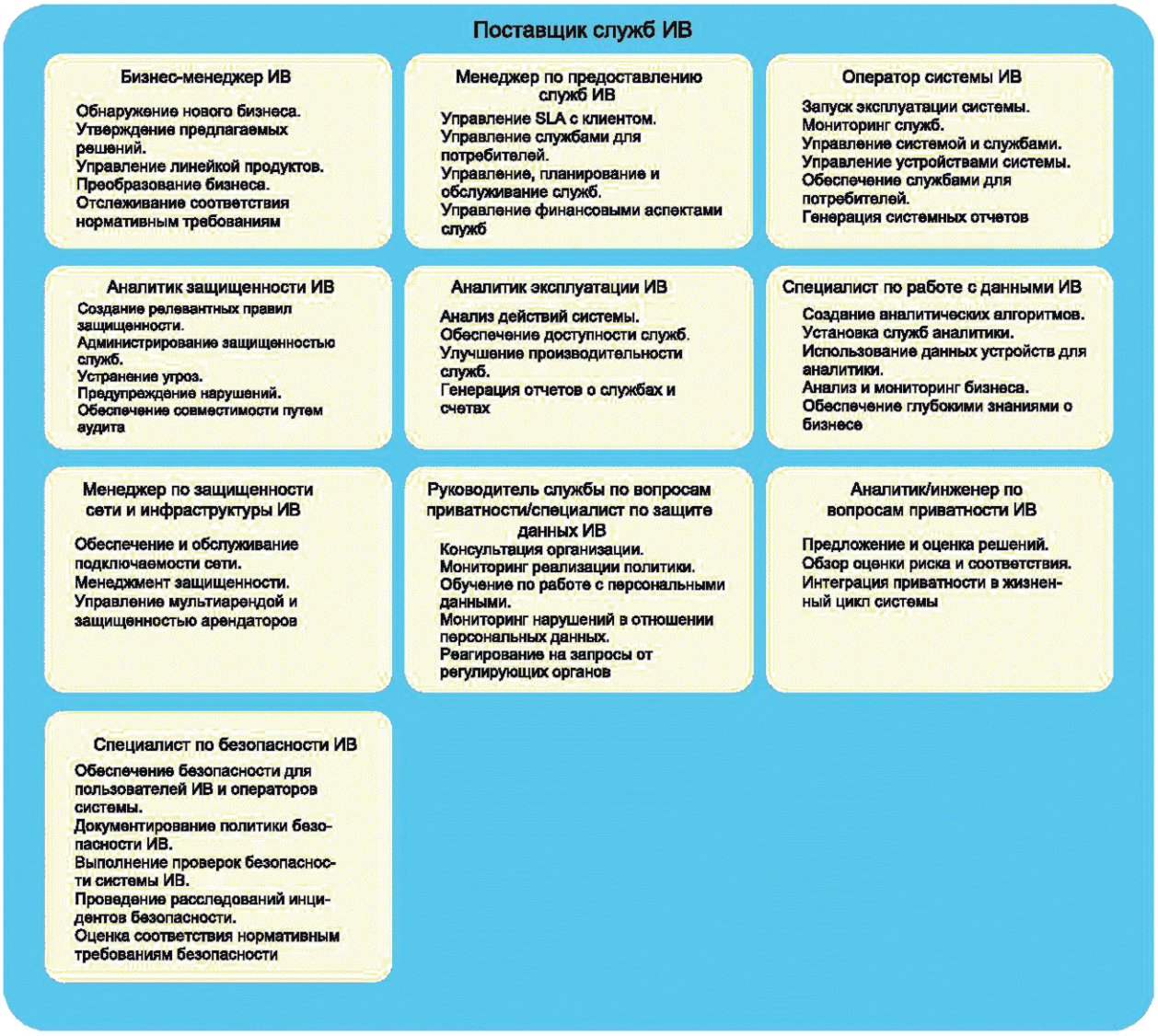

Рисунок 19 — Подроли и деятельности поставщика служб ИВ

10.5.2.3 Разработчик служб ИВ

Роли разработчика служб ИВ включают реализацию, тестирование и интеграцию служб ИВ в платформу ИВ. Разработчик служб ИВ включает следующие подроли:

- архитектор решения ИВ предлагает, проверяет и развертывает платформу ИВ в LOB. Архитектор выбирает стратегии и архитектуры интеграции для новой платформы ИВ, существующих бизнес-систем и устройств в производстве;
- менеджер процесса развертывания ИВ устанавливает, настраивает и ведет платформу ИВ и соответствующие службы, а также выступает в качестве менеджера проекта, поддерживая ИТ-службы для функционирования и разработки LOB;
- разработчик приложений ИВ работает в LOB, ИТ-отделе или с третьей стороной, разрабатывающей отраслевые приложения ИВ для LOB. Разработчик приложений ИВ использует возможности процесса развертывания для разработки, развертывания и восстановления приложений для интеграции устройств, данных и служб ИВ;
- разработчик устройств ИВ интегрирует аппаратное и программное обеспечение в устройства и приложения. Разработчик устройств ИВ устанавливает встроенное ПО, которое защищенным способом соединяет устройства с платформой ИВ;
- интегратор системы ИВ тестирует и интегрирует службы ИВ в платформу ИВ.

- руководитель службы по вопросам приватности/специалист по защите данных ИВ имеет следующие должностные обязанности (список является неполным): разработка новейших продуктов и служб с использованием больших данных при сохранении приватности, предложение и оценка решений для снижения рисков нарушения приватности (например, технологии, повышающие приватность), проведение оценки рисков нарушения приватности, проведение обзоров инцидентов безопасности и интеграция приватности на этапах жизненного цикла разработки программного обеспечения.

На рисунке 20 показаны подроли разработчика служб ИВ и их деятельности.



Рисунок 20 — Подроли и деятельности разработчика служб ИВ

10.5.2.4 Пользователь ИВ

Пользователь ИВ является конечным пользователем служб ИВ. Пользователь ИВ может быть пользователем-человеком или цифровым пользователем.

Пользователь-человек — это человек, который пользуется службами ИВ. Цифровые пользователи — это пользователи ИВ, не являющиеся людьми. Цифровые пользователи могут включать в себя службы автоматизации, которые действуют от имени пользователя-человека.

На рисунке 21 показаны все подроли пользователя ИВ и их деятельности.



Рисунок 21 — Подроли и деятельности пользователя ИВ

10.5.3 Сопоставление деятельностей, ролей и доменов систем ИВ

Представление использования рассматривает вопросы ожидаемого использования системы. На представлении использования отображаются роли и деятельности, позволяющие предоставлять поль-

зователям ИВ функциональность системы. Деятельности, которые создают, реализуют, тестируют, интегрируют и управляют службами ИВ в системах, могут потребовать взаимодействия между различными ролями (см. рисунок 19).

В таблице 2 представлены деятельности и соответствующие им роли.

Таблица 2 — Обзор деятельностей и подролей

Деятельности	Роли	Домены
Разработка устройств и приложений	Менеджер процесса развертывания ИВ. Разработчик устройств ИВ. Разработчик приложений ИВ	Домен приложений и служб. Домен восприятия и контроля
Работа с устройствами, подключаемостью и приложениями	Оператор системы ИВ. Менеджер по предоставлению служб ИВ	Домен эксплуатации и управления. Домен приложений и служб
Использование данных устройств для аналитики	Специалист по работе с данными ИВ. Аналитик защищенности ИВ. Аналитик эксплуатации ИВ	Домен эксплуатации и управления. Домен доступа и связи
Интеграция, работа и контроль с хранилищами данных и бизнесом	Архитектор решения ИВ. Менеджер процесса развертывания ИВ. Оператор системы ИВ. Интегратор системы ИВ. Менеджер по предоставлению служб ИВ	Домен приложений и служб. Домен эксплуатации и управления
Использование данных в режиме реального времени, архивных данных и больших данных для приложений и аналитики	Специалист по работе с данными ИВ. Аналитик эксплуатации ИВ. Аналитик защищенности ИВ. Менеджер по предоставлению служб ИВ	Домен приложений и служб. Домен эксплуатации и управления. Домен восприятия и контроля. Домен доступа и обмена ресурсами
Проведение и управление аналитикой для запуска бизнеса	Специалист по работе с данными ИВ. Аналитик эксплуатации ИВ. Разработчик приложений ИВ. Менеджер по предоставлению служб ИВ	Домен приложений и служб. Домен доступа и обмена ресурсами
Добавление аналитики на панель инструментов	Менеджер по предоставлению служб ИВ. Специалист по работе с данными ИВ. Разработчик приложений ИВ	Домен приложений и служб. Домен эксплуатации и управления. Домен доступа и обмена ресурсами
Мониторинг состояния системы, воздействие на риски защищенности и нарушения	Оператор системы ИВ. Аналитик защищенности ИВ	Домен эксплуатации и управления
Отслеживание соответствия нормативным требованиям	Бизнес-менеджер ИВ. Аналитик защищенности ИВ	Домен приложений и служб. Домен пользователей

На рисунках 22 и 23 показаны примеры использования систем ИВ с различными деятельностями.

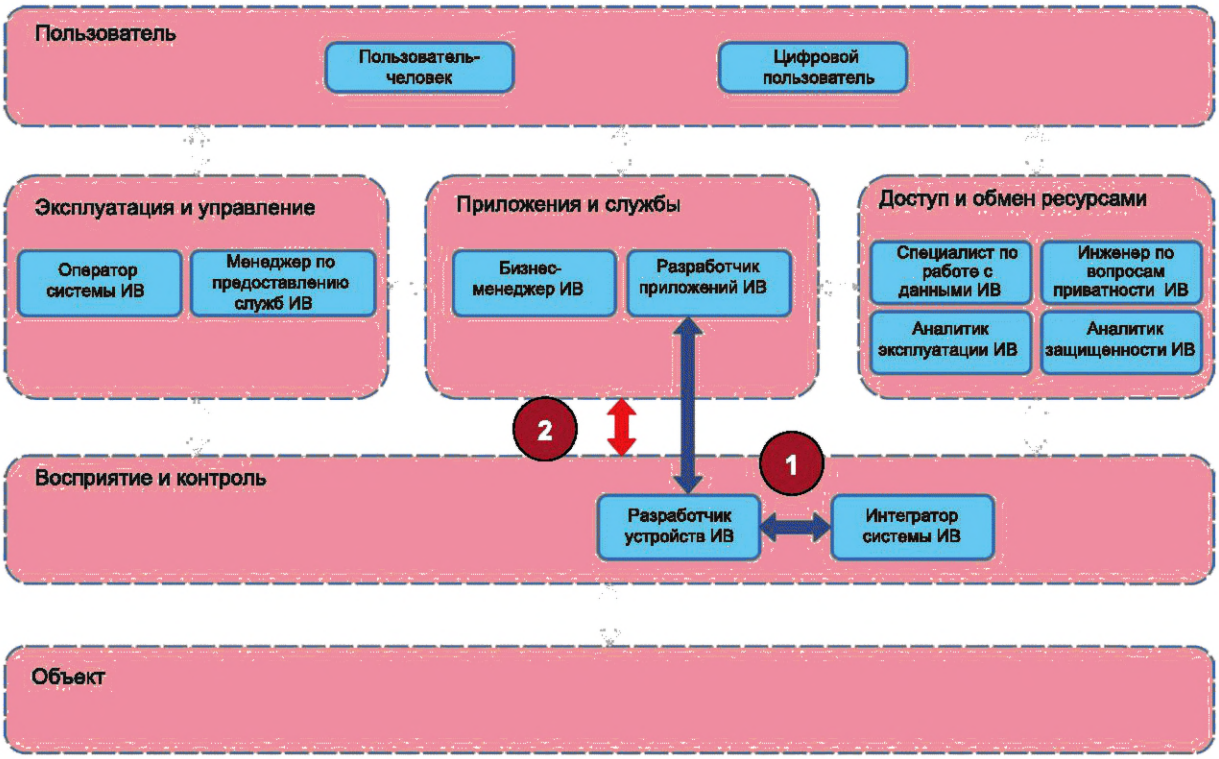

Рисунок 22 — Деятельности при разработке устройств и приложений

На рисунке 22 показаны деятельности и обмен информацией при разработке приложений устройств между разработчиками устройств, интеграторами системы и разработчиками приложений. Примером конкретной деятельности пользователя является подключение нового устройства к платформе ИВ. Система включает в себя следующие деятельности:

а) разработчик устройства взаимодействует с интегратором системы на этапе реализации. Они обсуждают определения API и функциональное поведение между устройством и платформой ИВ и согласовывают спецификацию;

б) разработчики приложений и разработчики устройств реализуют и тестируют API и их функции, связанные с устройством и платформой ИВ. На данном этапе устройства в домене восприятия и контроля подключаются к системам ИВ в домене приложений и служб, и конечные функции могут быть протестированы.

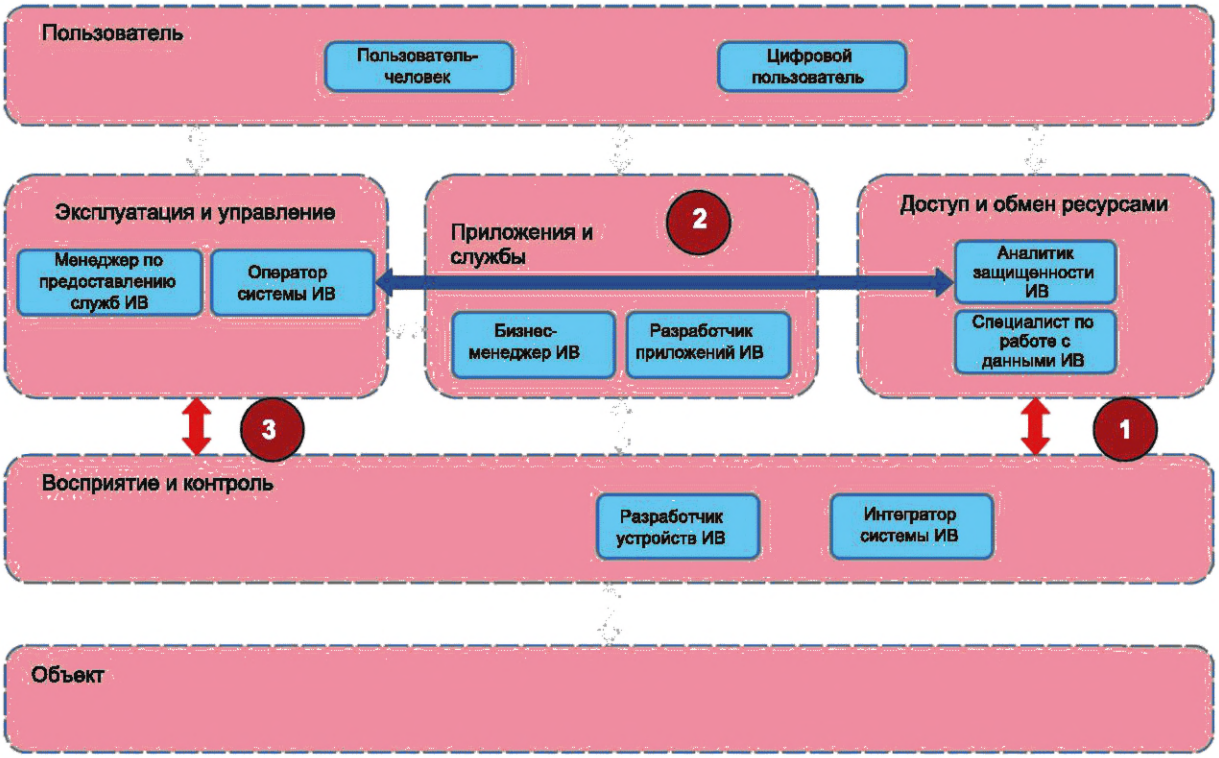

Рисунок 23 — Использование данных устройств для аналитики защищенности и эксплуатации

На рисунке 23 показан пример деятельностей, связанных с использованием данных устройств для аналитики защищенности и эксплуатации. Пользователями систем ИВ являются специалист по работе с данными и аналитик защищенности. Система включает в себя следующие деятельности:

а) после настройки и подключения устройства данные об использовании отправляются в домен доступа и обмена ресурсами системы ИВ. Аналитики защищенности и специалист по работе с данными используют собранные данные для проведения анализа защищенности;

б) аналитики защищенности взаимодействуют с операторами системы по результатам и выводам проведенного анализа;

в) аналитики защищенности и операторы системы совместно создают правила для защиты систем и предотвращения нарушений.

11 Доверенность системы ИВ

11.1 Общие положения

Доверенность систем ИВ включает в себя аспекты безопасности, защищенности, приватности и защиты персональных данных, способности к восстановлению и надежности. Данные аспекты представлены как междоменные возможности в функциональном представлении типовой архитектуры ИВ (см. 10.2). Данные аспекты являются междоменными, так как оказывают влияние на все домены и на большинство сущностей в системе ИВ.

В настоящем разделе определяется, как безопасность, защищенность, приватность и защита персональных данных, способность к восстановлению и надежность применяются к системам ИВ в контексте типовой архитектуры ИВ.

Аспекты доверенности определены в настоящем стандарте как свойства системы. Аспекты доверенности не являются набором межсистемных определенных функций. Доверенность всей системы можно рассматривать как набор независимых свойств, получаемых из доверенности ее подсистем и общей архитектурной и функциональной схемы. При выполнении основных функций система может не демонстрировать данные свойства, которые зависят от соглашений об уровне обслуживания или целей уровня обслуживания, а также от применяемых политик и нормативных правил. Данные свойства

являются предметом измерения, аудита и процедур подтверждения, которые включают в себя метрики, KPI и целевые показатели.

Необходимо проводить контроль характеристик доверенности в течение всего жизненного цикла системы ИВ. Характеристики доверенности должны рассматриваться интегрально как часть системы. Интегрированный подход необходим, поскольку аспекты доверенности влияют на систему не только в отдельности, но также друг на друга, положительно или отрицательно.

Каждый аспект доверенности должен быть изучен при проектировании, должен рассматриваться как неотъемлемая часть системы ИВ и должен быть встроен в ее конструкцию и функционирование.

Для каждой характеристики доверенности должна проводиться предварительная оценка, которая далее используется для определения требований к данному аспекту к системе ИВ. Для полного набора требований предварительная оценка дополняется политикой организации и бизнес-целями. Данный процесс должен учитывать компромиссы и взаимосвязь с другими характеристиками доверенности. Подсистема управления и эксплуатации обеспечивает элементы управления и механизмы для удовлетворения требований и их непрерывное применение в течение жизненного цикла системы ИВ.

Необходимо проводить мониторинг и измерение системы ИВ с помощью ряда KPI, которые разработаны и отражают данные, собранные из системы при ее работе. KPI могут быть использованы для диагностики работоспособности системы.

Не все характеристики доверенности могут иметь отношение к конкретной системе ИВ. Некоторые характеристики доверенности могут иметь первостепенное значение, а другие — вспомогательное. Например, во многих промышленных системах первостепенное значение имеют безопасность и надежность, остальные характеристики рассматриваются как дополнительные. На характеристики оказывают влияние отраслевые и региональные требования.

Как следствие, метрики и целевые показатели характеристик доверенности могут быть различными в зависимости от системы, отрасли промышленности или региона.

11.2 Безопасность

Безопасность определяется как состояние системы, работающей без причинения недопустимого риска травм или ущерба здоровью людей, прямого или косвенного в результате повреждения имущества или окружающей среды.

Безопасность включает в себя понятие функциональной безопасности. Функциональная безопасность относится к системам или оборудованию, функционирующих в ответ на все входные данные согласно ожиданиям. Первоочередной задачей безопасности являются корректирующие или предупреждающие действия, которые позволят избежать или уменьшить воздействие аварии.

Безопасность в системах ИВ включает в себя предотвращение вреда для людей, а также другим живым существам, окружающей среде и оборудованию.

Безопасность является главной проблемой многих систем ИВ, так как системы ИВ взаимодействуют с физическим миром и оказывают на него влияние. Такое вияние может нанести вред людям и другим живым существам, окружающей среде, оборудованию и другим физическим сущностям. Вред может быть нанесен из-за явных действий систем ИВ, например через управляющие запросы на исполнительные устройства. Вред также может быть нанесен из-за неявных действий, вызванных, например рекомендациями системы ИВ для пользователей-людей или ошибками и атаками на систему. Компоненты системы ИВ могут быть неисправны, в этом случае система ИВ должна обнаруживать и устранять такие сбои.

Все части и подсистемы системы ИВ должны обеспечивать безопасность, так как безопасность всей системы, как и другие характеристики доверенности, является производным свойством. Предупреждение вреда должно учитывать разные уровни, такие как физическое оборудование, напрямую контролируемое технологией ИВ, воздействие условий эксплуатации на операторов и косвенное воздействие на окружающую среду в долгосрочной перспективе.

Должна быть обеспечена система безопасности, касающаяся работы исполнительных устройств в системе ИВ, как в виде отдельных сущностей, так и в виде комбинированной системы.

С точки зрения безопасности должен рассматриваться весь жизненный цикл системы ИВ и должен быть установлен порядок действий при любых изменениях системы. Например, следует учитывать влияние на окружающую среду при утилизации оборудования или расходных материалов. Изменения системы могут включать в себя добавление в систему или изменение существующих частей. Любые изменения должны оцениваться с точки зрения безопасности.

11.3 Защищенность

11.3.1 Общие положения

Защищенность систем ИВ охватывает различные компоненты, включая в себя информационные системы, физические активы и продукты, производственные процессы, ОТ и оборудование.

11.3.2 Система менеджмента информационной безопасности (СМИБ) системы ИВ

Системы ИВ распределены и включают в себя большое количество разных сущностей, что образует большую поверхность атаки. Должны быть обеспечены надлежащие меры защищенности системы ИВ. *Вопросы информационной безопасности выходят за рамки положений настоящего стандарта и являются объектом стандартизации профильных национальных технических комитетов.*

Системы ИВ в большинстве случаев используют операционные технологии, которые включают в себя иной набор элементов по сравнению с информационными технологиями, безопасность которых обеспечивает традиционная СМИБ. В операционных технологиях делается акцент на вопросах физической защищенности, последствиях для безопасности и превентивных мерах. Сущности в домене восприятия и контроля могут быть изолированными путем неиспользования интернет-протоколов.

11.3.3 Типовая модель жизненного цикла безопасности системы и продукта ИВ

Как правило, организация, которая проводит разработку, передачу на стороннее исполнение или приобретение продукта системы ИВ, использует определенную структуру этапов процессов и деятельностей. Данная структура называется «моделью жизненного цикла». В зависимости от контекста структура называется «моделью жизненного цикла системы ИВ», «моделью жизненного цикла продукта ИВ» или «моделью жизненного цикла программного обеспечения». Модель жизненного цикла безопасности установлена в *ГОСТ Р ИСО/МЭК 12207* и *ГОСТ Р 57193*.

Модель жизненного цикла настраивается для конкретной организации. Экземпляром модели жизненного цикла является жизненный цикл системы или продукта ИВ, т. е. эволюция от концепции до вывода из эксплуатации. В разветвленных организациях различные группы могут использовать для проектов разные модели жизненного цикла системы ИВ. Некоторые организации разрабатывают специализированные модели жизненного цикла продуктов ИВ, например, web-продуктов ИВ, продуктов ИВ с режимом реального времени, встраиваемых продуктов ИВ, медицинских продуктов ИВ и т. д.

Деятельности на этапах жизненного цикла программного обеспечения или системы являются частью общеорганизационных процессов, которые должны удовлетворять требованиям *ГОСТ Р ИСО/МЭК 12207* и *ГОСТ Р 57193. ГОСТ Р 57102* и *ГОСТ Р 56923* определяют модели жизненных циклов разработки систем и программного обеспечения, этапы жизненного цикла и их взаимосвязи с процессами жизненного цикла.

Настоящий стандарт рекомендует дополнительно вводить деятельности «Меры и средства контроля и управления защищенности системы ИВ» (ISC) к деятельностям, выполняемым на этапах модели жизненного цикла продукта ИВ организации. Указанные деятельности должны быть адаптированы к используемой модели жизненного цикла с учетом характеристик разрабатываемой системы или продукта ИВ.

В настоящем стандарте представлена типовая модель жизненного цикла безопасности системы и продукта ИВ в качестве стандартизированной ссылки для добавления ISC к деятельностям, осуществляемым для управления продуктом ИВ, подготовки к работе и эксплуатации продукта ИВ, управления инфраструктурой и аудита продукта ИВ. Данная модель является представлением общих этапов и мероприятий, обычно присутствующих в моделях жизненного цикла продукта ИВ.

Типовая модель жизненного цикла безопасности системы и продукта ИВ не ограничивается разработкой программных средств. Она также затрагивает мероприятия из других сфер, таких как стратегическое управление, поддержка программных средств и инфраструктуры, управление проектами, аудит и контроль.

Цель типовой модели жизненного цикла безопасности системы и продукта ИВ состоит:

а) в содействии организации в подтверждении правильности каждой модели жизненного цикла системы и продукта ИВ путем определения всех процессов и действующих субъектов, потенциально вовлеченных в обеспечение защищенности продукта ИВ;

б) содействии организации в обеспечении уверенности в том, что вопросы безопасности надлежащим образом рассматриваются на всех этапах жизненного цикла продукта ИВ;

в) содействии организации в сведении к минимуму расходов и последствий от введения практических приемов согласно *ГОСТ Р ИСО/МЭК 27034-1* в ее проекты продуктов ИВ в качестве поддержки существующих моделей жизненного цикла продуктов ИВ;

г) предоставлении организации стандартной модели для коллективного использования ISC группами, занимающимися проектами продуктов ИВ, независимо от различных моделей жизненного цикла продуктов ИВ;

д) предоставлении организации стандартной модели для коллективного использования ISC вместе с другими организациями, независимо от различных моделей жизненного цикла продукта ИВ.

Графическое представление типовой модели жизненного цикла безопасности продукта ИВ показано на рисунке 24.

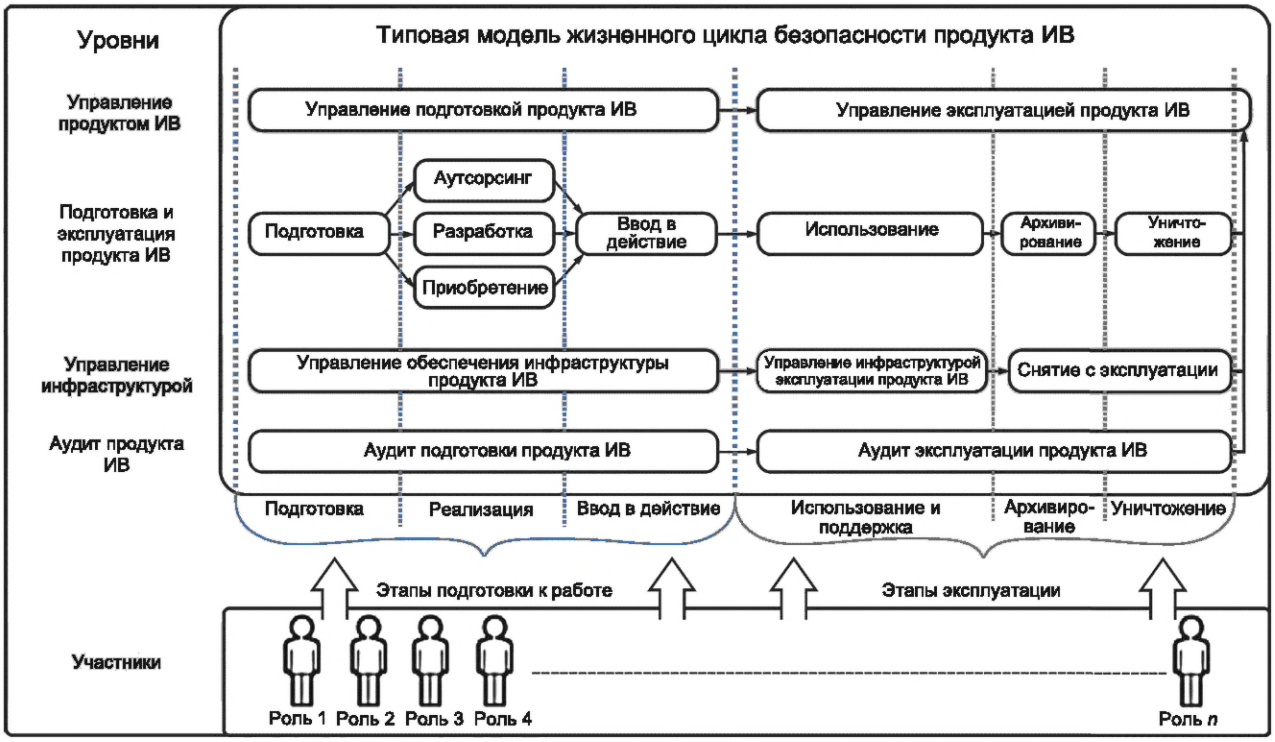

Рисунок 24 — Типовая модель жизненного цикла безопасности продукта ИВ

11.4 Приватность и защита персональных данных

Если система ИВ или часть системы ИВ собирает и обрабатывает персональные данные, то должна быть применена соответствующая защита персональных данных. Помимо обязательных требований по обеспечению безопасности персональных данных защита персональных данных является вопросом репутации и доверия к задействованной организации.

Не все системы ИВ собирают и обрабатывают персональные данные, например, традиционные системы производственных линий. Примером систем ИВ, которые включают в себя обработку персональных данных, являются домашние и медицинские системы ИВ.

Рекомендуется проводить PIA для системы ИВ, чтобы установить факт использования персональных данных в системе, и, при использовании, характеристики персональных данных и риски, связанные с обработкой персональных данных.

11.5 Надежность

Надежность — это способность системы ИВ или сущности в системе ИВ выполнять свои требуемые функции в установленных условиях в течение определенного периода времени.

Надежность может быть представлена различными метриками. В системах ИВ, где многие функции предоставляются в качестве службы различным агентам или другим компонентам, неотъемлемой частью определения надежности и доступности, в том числе эксплуатационной доступности, является качество обслуживания. Например, надежность сетевого компонента может определяться как стабильность обработки передачи данных в требуемых пределах скорости и задержки, что является формой доступности, включая эксплуатационную доступность. Доступность, в том числе эксплуатационная до-

ступность для облачной службы, может определяться на основе порогов качества, таких как допустимые пределы времени ответа.

В то время как способность к восстановлению — это способность системы реагировать на определенные неблагоприятные события, надежность характеризует гарантию использования и производительности системы. Надежность системы или службы напрямую зависит от способности к восстановлению ее подсистем или компонентов.

Неблагоприятные события обычно упоминаются в анализе способности к восстановлению, но также могут быть фактором надежности для лучшей оценки последствий использования. Целевые показатели надежности могут включать в себя следующие показатели ожидаемой частоты отказов или способности функционировать несмотря на отказы:

а) MTBF (среднее время между отказами) для ремонтируемой сущности, которое представляет собой ожидаемое время между последовательными отказами данной сущности;

б) MTTR (среднее время восстановления) для ремонтируемой сущности, которое представляет собой ожидаемую или наблюдаемую продолжительность возврата неисправной сущности к функционированию;

в) MTTF (среднее время до отказа) для неремонтируемой сущности, которое представляет собой среднее время выполнения функций сущностью до момента сбоя.

Надежность также зависит от других характеристик доверенности, таких как защищенность. Также может иметь влияние включение функций защищенности (таких как защита от вредоносных программ), установка исправлений или обновлений программного обеспечения или другие меры по усилению защиты системы. Негативные последствия, может иметь например неправильная установка обновлений или использование обновлений из неутвержденных или ненадежных источников.

Надежность системы и инфраструктуры ИВ. Общие требования:

а) не должно отрицательно влиять на включение функций защищенности;

б) должно быть управление уязвимостями для минимизации их влияния на надежность системы ИВ;

в) необходимо определить, способны ли средства управления обеспечить надежность и защищенность системы ИВ.

Национальные стандарты в области надежности — *ГОСТ Р МЭК 60300-1, ГОСТ Р 51901.5* и *ГОСТ Р 27.303.*

11.6 Способность к восстановлению

Способность к восстановлению — это способность системы быстро восстанавливать рабочее состояние после инцидента. Отказоустойчивость — это способность системы продолжать функционировать, когда в системе происходят повреждения, неисправности и сбои, потенциально ведущие к ухудшению возможностей системы. Надежность — это способность системы или компонента выполнять свои требуемые функции в указанных условиях в течение определенного периода времени.

Способность к восстановлению является важным фактором при проектировании и развертывании систем и инфраструктуры ИВ, поскольку влияет на бизнес-процессы. Требования к способности к восстановлению обосновываются аспектами безопасности, защищенности и надежности, а также бизнес-целями системы ИВ.

В аспекте способности к восстановлению допускается отказ отдельных сущностей, хотя он и является инцидентом, если система ИВ способна предоставлять свои возможности и поддерживается целостность этих возможностей. С практической точки зрения обеспечение способности к восстановлению включает в себя стратегию проектирования, которая направлена на уменьшение уязвимостей путем сокращения линий электропередачи, снижения избыточности в критических областях, укрепления локальных возможностей и решения проблемы зависимости и аварийного состояния.

Для системы ИВ должны быть установлены требования к способности к восстановлению и, как в случае с требованиями защищенности и приватности, это будет компромиссом между рисками и затратами, а также возможными компромиссами с другими аспектами доверенности. Некоторые требования к способности к восстановлению могут быть получены с учетом свойств безопасности, надежности или защищенности.

Управление устойчивостью проводится через определение рисков и угроз, которые необходимо уменьшать или противодействовать, что совпадает с подходом к защищенности. Управление устойчивостью начинается с оценки рисков и модели угроз. Стоимость рисков должна быть определена с точки

зрения прямых коммерческих издержек, а также с точки зрения влияния на систему, включая другие характеристики доверенности. Например, как отсутствие способности к восстановлению сети ближнего действия на периферии повлияет на надежность службы данных с точки зрения предоставления приложениям своевременных и точных данных. Далее должен быть определен требуемый уровень реагирования для каждого риска, необходимые контрмеры и их стоимость.

Областью ИВ, где допустима пониженная производительность во время сбоев, является оптимизация работы локальных компонентов управления системы ИВ (например, на предприятии) с использованием данных, собранных через Интернет (например, информации о погоде или местоположение и движение грузовиков, доставляющих комплектующие). Система может продолжать работать, даже если указанные внешние данные становятся недоступными в течение определенного периода (например, из-за сбоя связи). Даже если в этот момент работа системы ИВ не будет оптимальной, производственный процесс будет продолжен.

Таким образом, способность к восстановлению, как и другие элементы доверенности, требует анализа рисков и применения политик организации к этим рискам для определения наиболее подходящей конструкции системы.

Конструкция системы ИВ со способностью к восстановлению должна включать в себя несколько уровней избыточности, чтобы исключить отдельные точки отказа и максимизировать доступность возможностей системы ИВ. Конструкция должна включать в себя способы восстановления и понижения работы по мере необходимости. Такие способы включают в себя использование избыточных сущностей, модулей резервного копирования, резервных устройств и топологически избыточных путей. В конструкции должен быть использован набор методов обеспечения способности к восстановлению системы ИВ при атаках и сбоях сети. Между аспектами доверенности должен быть достигнут компромисс:

а) требования безопасности должны быть учтены при выборе стратегий проектирования способности к восстановлению. Способностью к восстановлению должна поддерживать требования безопасности;

б) неотъемлемой частью стратегии способности к восстановлению является защищенность. Должны быть учтены отказы блоков и компрометации устройств, шлюзов, систем обработки, сетей, сущностей хранения и обработки;

в) избыточность должна использоваться в максимально возможной степени;

г) должны использоваться легкоремонтируемые или легкозаменяемые компоненты, когда это возможно;

д) свойства и функции защищенности (шифрование, централизованная аутентификация и т. д.) должны быть реализованы таким образом, чтобы не оказывать отрицательного влияния на способность к восстановлению системы ИВ.

Требования в области способности к восстановлению — согласно *ГОСТ Р ИСО/МЭК 27031.*

11.7 Доверенность и типовая архитектура

Аспекты достоверности, рассмотренные в настоящем подразделе, не существуют изолированно и рассматриваются как ключевые факторы архитектуры систем ИВ. Каждый аспект имеет воздействия на систему, которые должны быть рассмотрены при проектировании и эксплуатации системы.

Требования безопасности имеют первостепенное значение. Распространенной является ситуация, когда управляющее программное обеспечение и службы размещаются рядом с исполнительными устройствами и датчиками с целью минимизации задействованной траектории. Это обеспечивает точное регулирование с минимумом задействованных элементов. Такое управляющее программное обеспечение должно быть разработано по принципу «безопасность в первую очередь» и направлено на устранение точечных отказов в других сущностях системы ИВ.

Для обеспечения защищенности требуются СМИБ, надлежащие меры защищенности во всей системе ИВ и оценка того, как устройства ИВ и системы, контролирующие устройства ИВ, могут быть защищены с использованием операционных технологий. Каждая сущность ИВ должна иметь соответствующие средства управления защищенности, и эти средства управления должны иметь возможность мониторинга и управления, в особенности с учетом необходимости обновлений в течение жизненного цикла системы ИВ.

Защита персональных данных требует идентификации сущностей ИВ, которые обрабатывают персональные данные. Система ИВ, обрабатывающая персональные данные, должна иметь элементы

системы управления персональными данными не только в виде централизованного компонента, но также в виде соответствующих элементов и средств управления для каждой сущности ИВ в системе.

Надежность требует соответствующей структуры системы для избегания единичных точек отказа. Избыточные или дублированные элементы и реплицированные наборы данных встраиваются в систему и процессы (автоматизированные) для устранения сбоев отдельных созданных сущностей. При разработке архитектуры должны быть учтены необходимость реализации и/или использования нескольких альтернативных версий программного обеспечения.

Общая надежность системы зависит как от надежности отдельных сущностей ИВ в системе, так и от общей архитектуры системы. Архитектура должна делать акцент на функциях, которые должна выполнять система, и обеспечивать конструкцию, которая дает соответствующие характеристики надежности для этих функций.

Для обеспечения способности к восстановлению требуется способность системы продолжать работать в условиях сбоев или атак, возможно, с пониженной производительностью.

Различные аспекты доверенности имеют индивидуальное влияние на систему, но также включают в себя взаимодействие друг с другом и компромиссы. Все указанные вопросы рассматриваются как часть проектирования системы, всего жизненного цикла и взаимосвязей между ними.

Приложение А
(справочное)

Интерпретация диаграммы классов UML для концептуальной модели

В настоящем стандарте диаграммы классов UML имеют следующие ограничения:

а) понятия представлены в виде классов UML без атрибутов;

б) документация для каждого понятия является определением понятия.

Используются два вида отношений:

- обобщение (отношение «является»): например, датчик является устройством ИВ. Пример отношения обобщения представлен на рисунке А.1;



Рисунок А.1 — Обобщение

- ассоциация. Наименование ассоциаций характеризуется действиями. На рисунке А.2 показано отношение ассоциации, когда датчик проводит мониторинг физической сущности (предмета).



Рисунок А.2 — Ассоциация

Ограничения количества элементов на концах ассоциации не показаны. Они варьируются от одного вида ассоциации к другому, но могут быть выведены из описаний.

Приложение В
(справочное)

Отношения сущностей концептуальной модели

В.1 Сущности и домены ИВ

Сущности и домены ИВ приведены в таблицах В.1—В.6.

Таблица В.1 — Сущность

Тип отношений	Наименование	Соответствующий элемент	Описание
Ассоциация	Имеет	Идентичность	Сущность имеет идентичность

Таблица В.2 — Домен

Тип отношений	Наименование	Соответствующий элемент	Описание
Ассоциация	Включает	Сущность	Домен включает одну или несколько сущностей
Ассоциация	Взаимодействует	Домен	Домен взаимодействует с другими доменами

Таблица В.3 — Цифровая сущность

Тип отношений	Наименование	Соответствующий элемент	Описание
Обобщение	Является	Сущность	Цифровая сущность является специализированной сущностью
Ассоциация	Содержит	Цифровая сущность	Цифровая сущность содержит другие цифровые сущности

Таблица В.4 — Физическая сущность

Тип отношений	Наименование	Соответствующий элемент	Описание
Обобщение	Является	Сущность	Физическая сущность является специализированной сущностью
Ассоциация	Содержит	Физическая сущность	Физическая сущность содержит другие физические сущности

Таблица В.5 — Пользователь ИВ

Тип отношений	Наименование	Соответствующий элемент	Описание
Обобщение	Является	Сущность	Пользователь ИВ является специализированной сущностью, представляющей пользователя-человека или цифрового пользователя

Таблица В.6 — Сеть

Тип отношений	Наименование	Соответствующий элемент	Описание
Обобщение	Является	Сущность	Сеть является специализированной сущностью

В.2 Идентификатор

Идентификатор приведен в таблице В.7.

Таблица В.7 — Идентификатор

Тип отношений	Наименование	Соответствующий элемент	Описание
Ассоциация	Идентифицирует	Сущность	Идентификатор идентифицирует сущность
Ассоциация	Отличает	Идентичность	Идентификатор отличает идентичность. Идентичность может иметь более одного идентификатора
Ассоциация	Идентифицирует	Контекст идентичности	Идентификатор идентифицируем в заданном контексте идентичности

В.3 Службы, сеть, устройства и шлюзы ИВ

Службы, сеть, устройства и шлюзы ИВ приведены в таблицах В.8—В.11.

Таблица В.8 — Оконечная точка

Тип отношений	Наименование	Соответствующий элемент	Описание
Ассоциация	Имеет	Интерфейс	Оконечная точка может содержать более одного интерфейса
Ассоциация	Существует в	Сеть	Оконечная точка существует в сети

Таблица В.9 — Шлюз ИВ

Тип отношений	Наименование	Соответствующий элемент	Описание
Ассоциация	Взаимодействует через	Сеть	Одна или несколько сетей, через которые осуществляются взаимодействия с другими сущностями
Ассоциация	Представляет	Оконечная точка	Одна или несколько оконечных точек, через которые осуществляются взаимодействия
Ассоциация	Использует	Хранилище данных	Нуль или более хранилищ данных использованы шлюзом ИВ
Ассоциация	Соединяет	Устройство ИВ	Одно или несколько устройств ИВ, соединенных через шлюз ИВ

Таблица В.10 — Устройство ИВ

Тип отношений	Наименование	Соответствующий элемент	Описание
Ассоциация	Взаимодействует через	Сеть	Одна или несколько сетей, через которые осуществляются взаимодействия с другими сущностями
Ассоциация	Представляет	Оконечная точка	Одна или несколько оконечных точек, через которые осуществляются взаимодействия
Ассоциация	Использует	Хранилище данных	Нуль или более хранилищ данных использованы шлюзом ИВ

Таблица В.11 — Служба

Тип отношений	Наименование	Соответствующий элемент	Описание
Ассоциация	Реализуется	Компонент	Служба реализуется одним или несколькими компонентами
Ассоциация	Представляет	Оконечная точка	Служба определяет интерфейсы сети и представляется оконечной точкой
Ассоциация	Взаимодействует через	Сеть	Служба взаимодействует через другие сущности через одну или несколько сетей
Ассоциация	Взаимодействует с	Шлюз ИВ	Служба взаимодействует с одним шлюзом ИВ или более
Ассоциация	Взаимодействует с	Устройство ИВ	Служба взаимодействует с одним устройством ИВ или более
Ассоциация	Взаимодействует с	Служба	Служба взаимодействует с одной службой или более
Ассоциация	Использует	Хранилище данных	Службой используется нуль или более хранилищ данных

В.4 Пользователь ИВ

Пользователи ИВ приведены в таблицах В.12—В.14.

Таблица В.12 — Пользователь-человек

Тип отношений	Наименование	Соответствующий элемент	Описание
Обобщение	Является	Пользователь ИВ	Пользователь-человек является специализированным пользователем ИВ
Ассоциация	Взаимодействует	Приложение	Пользователь-человек взаимодействует в сети через приложение

Таблица В.13 — Цифровой пользователь

Тип отношений	Наименование	Соответствующий элемент	Описание
Обобщение	Является	Пользователь ИВ	Цифровой пользователь является специализированным пользователем ИВ
Ассоциация	Взаимодействует	Приложение	Цифровой пользователь взаимодействует с одной или большим количеством служб, предлагаемых системой ИВ через сеть

Таблица В.14 — Приложение

Тип отношений	Наименование	Соответствующий элемент	Описание
Обобщение	Является	Служба	Приложение является службой

В.5 Виртуальная сущность, физическая сущность и устройство ИВ

Виртуальная, физическая сущность и устройство ИВ приведены в таблицах В.15—В.17.

Таблица В.15 — Датчик

Тип отношений	Наименование	Соответствующий элемент	Описание
Обобщение	Является	Устройство ИВ	Датчик является специализированным устройством ИВ
Ассоциация	Проводит мониторинг	Физическая сущность	Датчик проводит мониторинг физической сущности

Таблица В.16 — Исполнительное устройство

Тип отношений	Наименование	Соответствующий элемент	Описание
Обобщение	Является	Устройство ИВ	Исполнительное устройство является специализированным устройством ИВ
Ассоциация	Воздействует	Физическая сущность	Исполнительное устройство воздействует на физическую сущность

Таблица В.17 — Виртуальная сущность

Тип отношений	Наименование	Соответствующий элемент	Описание
Ассоциация	Взаимодействует	Оконечная точка	Виртуальная сущность взаимодействует через оконечную точку
Ассоциация	Представляет	Физическая сущность	Виртуальная сущность представляет физическую сущность

Приложение С
(справочное)

Отношение между концептуальной моделью, типовой моделью и типовой архитектурой

С.1 Типовая модель — это абстрактная структура для понимания значимых связей между сущностями среды и для разработки согласованных стандартов или спецификаций, поддерживающих эту среду. Типовая модель основана на небольшом числе объединяющих понятий и может использоваться в качестве основы для обучения и объяснения стандартов неспециалистам.

Типовая модель не связана напрямую с какими-либо стандартами, технологиями или конкретными деталями реализации, а обеспечивает базовое понимание.

Ряд понятий является частью типовой модели. Типовая модель является абстрактной и предоставляет определенную информацию об окружающей среде. Типовая модель описывает тип сущностей, которые встречаются в такой среде, а не конкретные сущности в конкретной среде. Типовая модель описывает типы сущностей и доменов и их отношения. Типовая модель описывает не обязательно все сущности в структуре, а только необходимые для конкретной ситуации.

Типовая модель используется для:

- создания стандартов для объектов модели и их взаимосвязей;
- обучения третьей стороны;
- определения четких ролей и обязанностей в системе;
- сравнения разных сущностей.

С.2 Под типовой архитектурой понимаются контексты, снабженные общими характеристиками, лексиконом, требованиями и вспомогательными элементами. Вспомогательными элементами является описание основных компонентов базовой архитектуры с предоставлением рекомендаций и ограничений для создания экземпляров архитектур решений. Архитектуры решения могут быть определены с разных точек зрения и на многих разных уровнях детализации и абстракции. Архитектуры решения включают в себя список сущностей, функции, соединения, взаимосвязи и взаимодействия друг с другом и с функциями, расположенными вне предопределенных архитектурных шаблонов. На рисунке С.1 показана последовательность архитектуры от концептуальной модели до типовой модели на основе сущностей и типовой модели на основе доменов для ряда различных представлений типовой архитектуры. Порядок в последовательности архитектуры может отличаться от указанного и быть «эволюционным». Описания архитектуры должны быть задокументированы. На основе концептуальной модели разработана типовая модель на основе сущностей для демонстрации взаимосвязи между системами ИВ на высоком уровне. Концепция доменов позволяет разделить разработку архитектур ИВ для конкретных решений. Типовая модель на основе доменов является основой для дальнейшей декомпозиции и разработки представлений архитектуры.

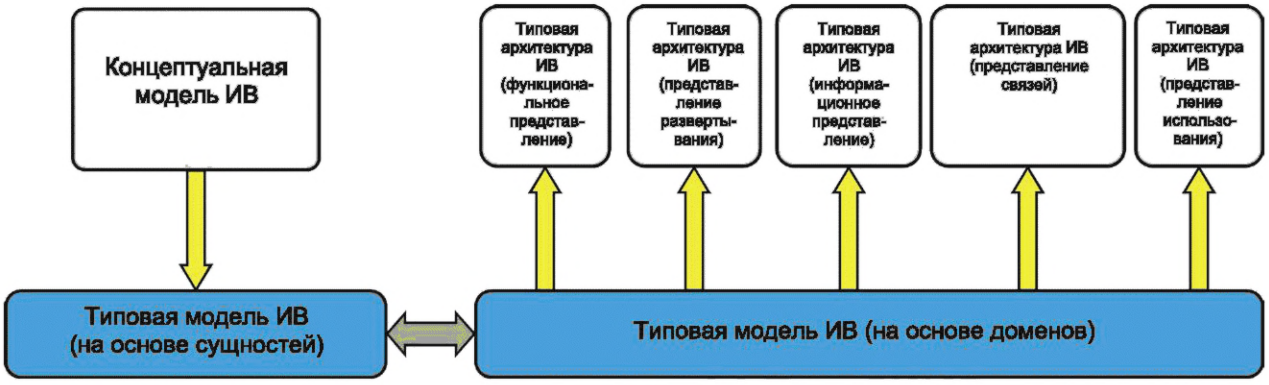

Рисунок С.1 — Взаимосвязи между концептуальной моделью, типовой моделью и типовой архитектурой

Домены систем ИВ определяются путем изучения заинтересованных сторон и аппаратного и программного обеспечения систем ИВ. Использование общих и репрезентативных доменов обеспечивает эффективную и актуальную типовую модель систем ИВ для различных целей и применений типовой модели.

Библиография

[1] ИСО/МЭК 20924:2018 Информационные технологии. Интернет вещей. Термины и определения

УДК 004.738:006.354 ОКС 35.110

Ключевые слова: информационные технологии, интернет вещей, типовая архитектура, типовая модель

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *С.И. Фирсова*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 28.11.2023. Подписано в печать 13.12.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 7,44. Уч.-изд. л. 6,72.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru