Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1257

(03/2016)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Управление определением идентичности

Таксономия управления определением идентичности и управления доступом

Рекомендация МСЭ-Т X.1257

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	**X.1250–X.1279**
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1257

Таксономия управления определением идентичности и управления доступом

Резюме

В Рекомендации МСЭ-Т X.1257 разработана спецификация, обеспечивающая присвоение необходимого бизнес-значения ролям и разрешениям управления определением идентичности и управления доступом (IAM), а также прослеживаемость этого бизнес-значения и возможность ссылки на него на протяжении всего жизненного цикла процесса IAM. Это означает, что возможно эффективное присвоение пользователям разрешений, успешная реализация средств управления разделением обязанностей (SoD) по приложениям и эффективное выполнение процессов пересмотра и согласования прав доступа.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1257	23.03.2016 г.	17-я	11.1002/1000/12608

Ключевые слова

Управление доступом, жизненный цикл IAM, управление определением идентичности и доступом, роль, разрешение, бизнес-значение, бизнес-таксономия, бизнес-задача.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например: http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1257

Таксономия управления определением идентичности и управления доступом

1 Сфера применения

В настоящей Рекомендации определяются требования к присвоению бизнес-значения ролям управления определением идентичности и управления доступом (IAM) и разрешений пользователям с использованием [ITU-T X.1252], [ITU-T X.1254] и [b-ITU-T X.1255] и расширению этих требований, с тем чтобы предложить следующее:

- таксономию IAM для семантического определения и организации этапов и процессов IAM в целях представления полного жизненного цикла процесса IAM;
- онтологическую модель IAM для семантического определения типов ролей и разрешений IAM, их синтаксиса и соответствующих отношений типов.

2 Справочные документы

Нижеследующие Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые, путем ссылок на них в данном тексте, составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники являются предметом пересмотра; поэтому всем пользователям данной Рекомендации предлагается рассмотреть возможность применения последнего издания Рекомендаций и других ссылок, перечисленных ниже. Перечень действующих на текущий момент Рекомендаций МСЭ-Т публикуется регулярно. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности.*

[ITU-T X.1254] Рекомендация МСЭ-Т X.1254 (2012 г.), *Структура гарантии аутентификации объекта.*

3 Определения

3.1 Термины, определенные в других документах

3.1.1 контроль доступа (access control) [ITU-T X.1252]: Процедура, применяемая для определения того, следует ли предоставлять тому или иному объекту доступ к ресурсам, устройствам, услугам или информации на основе заранее установленных правил и конкретных прав или полномочий, связанных с запрашивающей стороной.

3.1.2 атрибут (attribute) [ITU-T X.1252]: Информация, связанная с объектом, которая означает какую-либо его характеристику.

3.1.3 контекст (context) [ITU-T X.1252]: Среда с определенными граничными условиями, в которой существуют и взаимодействуют объекты.

3.1.4 регистрационные данные (credential) [ITU-T X.1252]: Набор данных, представляемых как доказательство заявляемой идентичности и/или предоставленных прав.

3.1.5 объект (entity) [ITU-T X.1252]: Что-либо, что существует отдельно и обособленно и может быть определено в контексте.

3.1.6 идентификатор (identifier) [ITU-T X.1254]: Один или несколько атрибутов, которые однозначно характеризуют объект в конкретном контексте.

3.1.7 идентичность (identity) [b-ISO/IEC24760-1]: Набор атрибутов, связанных с объектом.

ПРИМЕЧАНИЕ. − В конкретном контексте идентичность может содержать один или несколько идентификаторов, которые позволяют однозначно распознать объект в данном контексте.

3.1.8 роль (role) [ITU-T X.1252]: Комплекс свойств или атрибутов, которые описывают возможности или функции, обеспечиваемые объектом.

ПРИМЕЧАНИЕ. − Каждый объект может иметь/выполнять много ролей. Возможности могут быть изначальными или приобретенными.

3.1.9 пользователь (user) [ITU-T X.1252]: Любой объект, использующий ресурс, например систему, оконечное оборудование, процесс, приложение или корпоративную сеть.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 предоставление доступа (access assignment): Процесс присвоения прав доступа пользователю (пользователям).

3.2.2 управление запросами на изменение прав доступа (access change request management): Процесс управления запросами на изменение прав доступа.

3.2.3 ограничения доступа (access constraints): Набор ограничений доступа на основании местоположения пользователя, временных ограничений на выполняемые задачи и временных ограничений на ресурсы.

3.2.4 организация доступа (access engineering): Процесс создания и сопровождения прав доступа.

3.2.5 осуществление доступа (access operation): Процесс оценки прав доступа пользователя в целях выполнения определенных задач.

3.2.6 политика доступа (access policy): Ограничительный механизм контроля доступа (т. е. определение бизнес-разрешений, которые пользователь может использовать в течение рабочего цикла).

3.2.7 согласование доступа (access reconciliation): Процесс изменения прав доступа пользователя в соответствии с установленными требованиями к правам доступа во избежание предоставления пользователю доступа с избыточными (или недостаточными) привилегиями.

3.2.8 пересмотр прав доступа (access review): Процесс пересмотра прав доступа пользователя в целях последующего согласования и сертификации доступа.

3.2.9 политика присвоения (assign policy): Ограничительный механизм присвоения разрешений (т. е. определение задач, которые могут быть назначены пользователю).

3.2.10 организация логики авторизации (authorization logic engineering): Процесс разработки и сопровождения логики авторизации в соответствующих приложениях.

3.2.11 браузер (browser): Приложение, запускаемое на устройстве, которое применяет пользователь для взаимодействия с поставщиком услуг.

3.2.12 бизнес-роль (business role): Набор задач (при наличии или в отсутствие разрешений), которые пользователь иметь право выполнять.

3.2.13 регистрация для доступа к бизнес-задачам (business task access logging): Процесс регистрации успешно завершенного выполнения задачи или факта отсутствия у пользователя разрешения на выполнение определенных(ой) задач(и).

3.2.14 авторизация выполнения бизнес-задачи (business task execution authorization): Процесс авторизации пользователя для выполнения конкретной бизнес-задачи на конкретном ресурсе.

3.2.15 выполнение бизнес-задачи (business task execution): Процесс выполнения конкретных(ой) задач(и).

3.2.16 организация бизнес-таксономии (business taxonomy engineering): Процесс создания и сопровождения таксономии бизнес-процессов и бизнес-продуктов.

3.2.17 таксономия бизнес-процессов (business process taxonomy): Таксономия, семантически определяющая и организующая бизнес-процессы и субпроцессы в иерархическую структуру.

3.2.18 канал (channel): Способ связи, выбранный пользователем для взаимодействия с поставщиком услуг.

3.2.19 устройство (device): Механизм, применяемый пользователем для обеспечения возможности взаимодействия с поставщиком услуг.

3.2.20 предоставленное право (entitlement): Набор задач и разрешений, назначенных пользователю.

3.2.21 жизненный цикл процесса IAM (IAM process lifecycle): Жизненный цикл процессов и субпроцессов управления определением идентичности и управления доступом (IAM).

3.2.22 организация ролей IAM (IAM role engineering): Процесс создания и сопровождения ролей и разрешений IAM.

3.2.23 намерение (intent): Основание или причина, обусловливающие инициирование пользователем взаимодействия с поставщиком услуг.

3.2.24 разрешение (permission): Набор бизнес-ресурсов для доступа к задачам (задаче), ограниченный соответствующей политикой контроля доступа.

3.2.25 ресурс (resource): Оконечный узел таксономии бизнес-продуктов, который также называется бизнес-продуктом.

3.2.26 сеанс (session): Блок атрибутов аутентификации и авторизации в течение времени выполнения.

3.2.27 задача (task): Оконечный узел таксономии бизнес-процессов, который также называется бизнес-задачей.

3.2.28 группа (team): Блок бизнес-ролей людских ресурсов, которые совокупно имеет каждый член группы.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

APQC	American Productivity and Quality Center	Американский центр проблем повышения производительности и качества продукции
CPC	Central Product Classification	Классификация основных продуктов
eTOM	Enhanced Telecom Operations Map	Расширенная карта бизнес-процессов оператора электросвязи
HTTP	HyperText Transfer Protocol	Протокол передачи гипертекста
IAM	Identity and Access Management	Управление определением идентичности и управление доступом
IP	Internet Protocol	Протокол Интернет
IT	Information Technology	Информационные технологии
JSON	JavaScript Object Notation	Нотация объектов JavaScript
JSON-LD	JSON-based Serialization for Linked Data	Сериализация связанных данных на базе JSON
MAC	Media Access Control	Управление доступом к среде передачи
PCF	Process Classification Framework	Структура классификации процессов
RBAC	Role Based Access Control	Управление доступом на основе ролей
REST	Representational State Transfer	Передача репрезентативного состояния
SCIM	System for Cross-domain Identity Management	Система междоменного управления определением идентичности
SDLC	Software Development Life Cycle	Жизненный цикл разработки программного обеспечения
SKOS	Simple Knowledge Organization System	Простая система организации знаний

SOAP	Simple Object Access Protocol	Простой протокол доступа к объектам
SoD	Separation of Duties	Разделение обязанностей
URL	Uniform Resource Locator	Унифицированный указатель ресурса
XACML	eXtensible Access Control Markup Language	Расширяемый язык разметки контроля доступа

5 Условные обозначения

В настоящей Рекомендации используются следующие условные обозначения:

Слово с прописной буквы в середине предложения означает использование термина, который является частью модели (т. е. модели онтологии IAM или модели таксономии IAM), например "Бизнес-роль" или "Организация ролей IAM", и который также встречается в соответствующих схемах. Термины "бизнес-задача" и "задача" используются равнозначно в целях удобства чтения. Термины "бизнес-ресурс" и "ресурс" используются равнозначно в целях удобства чтения.

6 Введение

Отсутствие общепринятого бизнес-значения существующих в настоящее время ролей управления определением идентичности и управления доступом (IAM) и разрешений пользователя негативно влияет на весь жизненный цикл IAM. На многих предприятиях широко применяются такие роли IAM, как "SuperAdmin", "SuperUpdate" и "XYZSystemSpecialAccess", несмотря на то что их значения неоднозначны, чересчур техничны и неясны. Естественно, что вместо использования таких неоднозначных ролей инженер по организации ролей IAM будет вновь и вновь создавать новые роли. В итоге это приведет к большому количеству трудно управляемых и предназначенных для конкретной системы ролей IAM, которые не передают изначально предусмотренного для них бизнес-значения.

Такое большое количество ролей, а также их низкое семантическое качество негативно влияют на основные этапы жизненного цикла IAM, такие как Предоставление доступа, Авторизация доступа, Пересмотр прав доступа и Согласование доступа. При Предоставлении доступа специалист по управлению доступом, не понимающий значения существующих ролей, может присвоить пользователю неверные привилегии. Для того чтобы компенсировать нечеткость бизнес-значения ролей IAM, разработчикам приложений приходится жестко программировать логику авторизации в своих приложениях. Синхронизация сопровождения такого исходного кода логики авторизации в приложениях проблематична и чревата ошибками. Кроме того, трудно (если вообще возможно) реализовать средства управления для Разделения обязанностей (SoD) между разными приложениями. При Пересмотре прав доступа ввиду того же отсутствия бизнес-значения ролей IAM, а также необходимости соблюдения предельных сроков специалисты по пересмотру прав доступа ошибочно сертифицируют (или отзывают) права доступа пользователей. Высокий показатель таких ошибок пересмотра прав и чреватая ошибками реализация логики авторизации повышают риск причинения ущерба репутации и финансовых потерь, ставят под вопрос нормативно-правовое соответствие, отрицательно влияют на производительность работы группы IAM и ограничивают возможности по созданию крупномасштабных корпоративных решений, таких как оптимизация процессов, приложений и ролей.

В силу того что текущие стандартные спецификации контроля доступа не определяют семантику ролей и разрешений IAM, необходимо выработать дополнительный набор требований к управлению доступом. Такие требования будут гарантировать присвоение ролям и разрешениям IAM необходимого бизнес-значения, а также прослеживаемость этого бизнес-значения и возможность ссылок на него на протяжении всего жизненного цикла процесса IAM, чтобы было возможно эффективное присвоение пользователям разрешений, успешная реализация средств управления разделением обязанностей (SoD) по приложениям и эффективное выполнение процессов пересмотра и согласования прав доступа.

7 Обзор подхода

Учитывая, что сферой применения настоящей Рекомендации является разработка набора требований по присвоению бизнес-значения ролям IAM, ниже приводится подробное описание подхода. Как было отмечено в разделе 6, группа по организации ролей IAM должна присваивать новым ролям IAM требуемое бизнес-значение. Однако каков источник такого бизнес-значения и кто может его разработать? Сегодня бизнес-архитекторы вооружены бизнес-стратегией и перед ними поставлена задача разработки таксономии бизнес-процессов и бизнес-продуктов.

Таксономия бизнес-процессов семантически определяет и организует бизнес-процессы и субпроцессы в иерархическую структуру (в целях навигации по составляющим процесса), которая начинается с Отрасли, являющейся корнем этой структуры, и состоит из Бизнес-области, Бизнес-процесса, Бизнес-действия и Бизнес-задачи (более подробно см. в Дополнении VI "Стандарты таксономии бизнес-процессов"). Бизнес-таксономия также включает в себя иерархию бизнес-продуктов и ее обычно составляют и ведут архитекторы бизнес-продуктов в форме большой электронной таблицы или файла документа.

В течение жизненного цикла разработки программного обеспечения (SDLC) фрагменты содержания такой иерархии копируются и вставляются бизнес-аналитиками для составления документов, содержащих бизнес-требования, которые передаются для дальнейшей реализации группе организации ролей IAM и группе разработчиков приложений. Инженер по ролям не может обращаться к конкретным бизнес-задачам по их идентификатору, в силу чего он обычно создает роли IAM – с определением или без него – в соответствии со своей устаревшей интерпретацией задач, которые может выполнять пользователь. В результате бизнес-значение роли IAM утрачивается или неправильно понимается разработчиком приложения. Каким образом можно разрешить эту проблему?

Для того чтобы разрешить эту проблему, необходимо обеспечить возможность ссылки на бизнес-значение ролей IAM и его прослеживаемости до соответствующих текущих бизнес-задач на протяжении всего жизненного цикла процесса IAM. Это фундаментальная качественная характеристика, которая может повысить качество всего жизненного цикла процесса IAM. Каким образом можно реализовать эту качественную характеристику? Существует ряд подходов на основе семантического представления для реализации интерфейса прикладного программирования бизнес-таксономии (см. Дополнение V "Возможные механизмы реализации интерфейса бизнес-таксономии").

Однако одной возможности ссылки на бизнес-значение и его прослеживаемости на протяжении жизненного цикла процесса IAM недостаточно. Необходимо также определить семантический синтаксис ролей IAM.

В настоящее время синтаксис ролей IAM определяется широко распространенным стандартным механизмом контроля доступа, называемым "Управление доступом на основе ролей" (RBAC), иллюстрация которого приведена на рисунке 1.

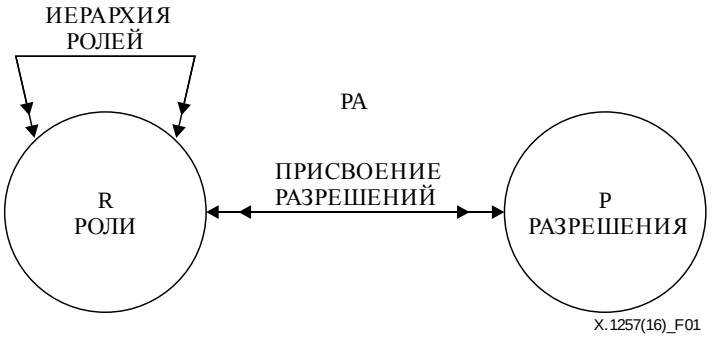

Рисунок 1 − Традиционная модель RBAC

Эта схема поясняет следующий синтаксис ролей:

- роли могут содержать другие роли, т. е. формируется иерархия ролей;
- роли состоят из разрешений.

Однако такой традиционный механизм RBAC имеет известное ограничение – он не определяет семантику разрешений (т. е. "природу разрешений"). Вместо этого спецификация оставляет семантику разрешений открытой для толкования – "разрешения могут определяться в терминах элементарных операций, таких как чтение и запись, или абстрактных операций, таких как кредит и дебет" [b-NIST-RBAC 2000]. Однако на практике, как показано в разделе 6, создаются неоднозначные роли IAM без ссылок на соответствующие бизнес-задачи.

Для того чтобы ролям IAM можно было присваивать бизнес-значение, требуется определить семантический синтаксис ролей IAM. Значения будут определяться по наиболее мелким оконечным узлам бизнес-таксономии – задачам и ресурсам. Семантический синтаксис роли IAM показан на рисунке 2.

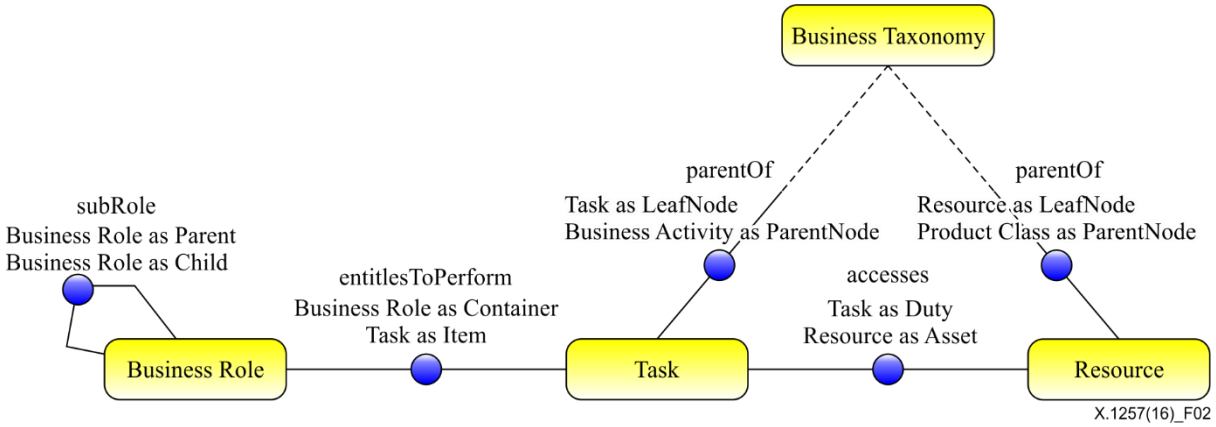

Рисунок 2 − Управление доступом на основе задач, концептуальная схема

Из этой схемы следует, что:

- роли (по-прежнему) могут содержать другие роли через отношение "Суброль" (subRole), т. е. формировать иерархию ролей;
- основной семантический синтаксис ролей IAM:
  - бизнес-роль обеспечивает пользователю право выполнять бизнес-задачи(у) через отношение "имеет право Выполнять" (entitlesToPerform). Это позволяет любой роли IAM неявно наследовать свое бизнес-значение от соответствующих бизнес-задач;
  - бизнес-задача (не пользователь или роль) осуществляет доступ к определенному ресурсу (т. е. "Бизнес-продукту"). Отношение "осуществляет доступ" (accesses) не является обязательным и необходимо в ситуациях, когда требуется контроль доступа с более детальной разбивкой;
  - задача и ресурс как оконечные узлы бизнес-таксономии служат основными конструктивными блоками при организации ролей IAM, и на протяжении всего жизненного цикла процесса IAM на них делаются ссылки.

Для простоты родительские типы продуктов задач и ресурсов на рисунке 2 не показаны.

В таблице 1 приведены несколько примеров предоставленных прав с применением вышеописанного синтаксиса, которые помогут проиллюстрировать вышеизложенное.

Таблица 1 − Пример предоставленных прав

Бизнес-роль	Задача	Ресурс
Банковский служащий	Открытие счета	Расширенный текущий счет
Врач	Изучение истории болезни	История болезни
Системный администратор	Обновление системной среды	Системная среда

Приведенный выше семантический синтаксис ролей IAM достигает главной цели – присвоение ролям IAM бизнес-значения. В следующем разделе предлагаемый подход представлен в формате требований.

8 Требования к семантике и синтаксису IAM

Для того чтобы роли IAM имели необходимое бизнес-значение, вводятся следующие рекомендации.

1) Бизнес-таксономия служит необходимым условием жизненного цикла процесса IAM, обеспечивая бизнес-значение ролей IAM и разрешения пользователям на протяжении всего жизненного цикла.

2) На бизнес-значение ролей IAM могут делаться ссылки и оно может прослеживаться до соответствующих бизнес-задач бизнес-таксономии на протяжении жизненного цикла процесса IAM.

3) К ролям IAM применяется следующий семантический синтаксис.

   3.1) Роль IAM состоит из бизнес-задач, которые пользователь имеет право выполнять.

   3.2) Роль IAM состоит из бизнес-задач, которые необязательно осуществляют доступ к конкретным бизнес-ресурсам, если требуется контроль доступа с более детальной разбивкой.

4) Успешное выполнение бизнес-задач, а также запросы на несанкционированное выполнение бизнес-задач должны регистрироваться путем ссылок на соответствующие идентификаторы бизнес-задач.

Приложение A

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Данное Приложение оставлено пустым и предназначено для представления возможных будущих сценариев реализации управления доступом на основе задач IAM.

Дополнение I

Жизненный цикл процесса таксономии IAM

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Рисунок I.1 иллюстрирует тот факт, что на весь жизненный цикл процесса IAM воздействуют в первую очередь изменения в бизнес-таксономии. Эти изменения в бизнес-таксономии прописываются и используются группами по организации ролей IAM и организации логики авторизации. Изменения содержат идентификаторы бизнес-задач в соответствующих артефактах, таких как роли IAM, исходный код Логики авторизации и файлы журналов регистрации выполнения и авторизации для выполнения бизнес-задач.

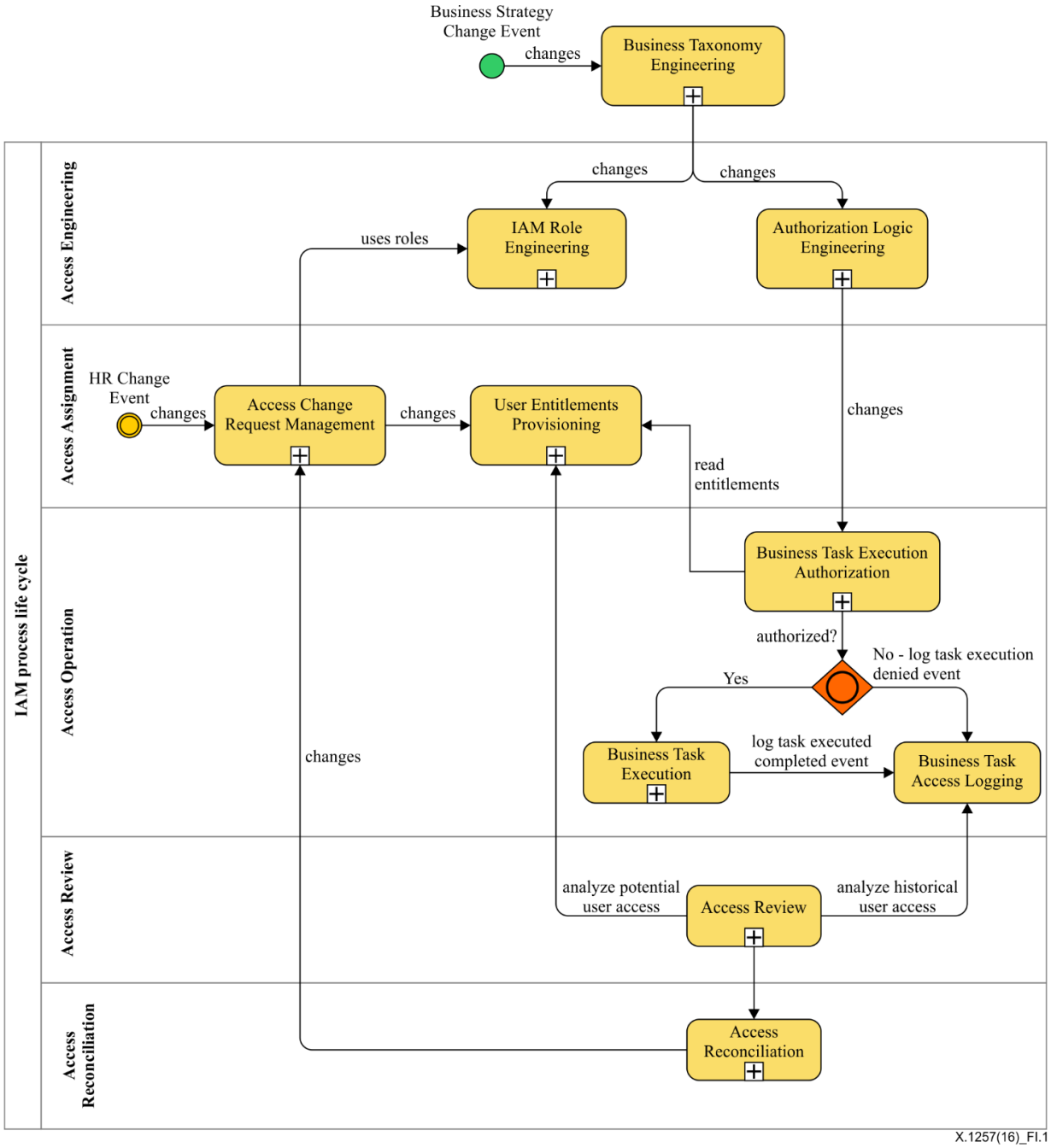

Рисунок I.1 – Зависимости жизненного цикла процесса IAM

Вторым источником изменений являются события, связанные с людскими ресурсами, такие как наем, отпуск, перевод и другие подобные события. Эти события обрабатываются процессом Управление запросами на изменение прав доступа, и в каталогах предоставленных прав пользователей прописываются соответствующие предоставленные права пользователя. В частности, эти предоставленные права будут содержать ссылки на идентификаторы бизнес-задач, которые обеспечивают бизнес-значение, и далее на них будут делаться ссылки при авторизации для выполнения приложения. После аутентификации пользователя (для простоты этот процесс не показан) средства предупредительного управления SoD в процессе авторизации для выполнения будут блокировать выполнение бизнес-задач, не совместимых с правами пользователя. В процессе Авторизации для выполнения бизнес-задачи пользователь либо получает разрешение на выполнение задачи и задача выполняется, либо же пользователь не получает разрешения на выполнение задачи. В обоих случаях приложение регистрирует эти события, ссылаясь на соответствующие идентификаторы бизнес-задач. Ниже приведен возможный пример формата журнала регистрации:

```
2016-02-08 22:20:02,165 ait:AppID1 192.168.0.1 UserID123 btt:TaskID1 btr:456:355 bttes:200 "Task successfully completed."

2016-02-08 22:24:02,165 ait:AppID1 192.168.0.1 UserID123 btt:TaskID2 bttes:401 "User Not Authorized to execute Task",
```

где:

- **btt** – пространство имен, которое разрешается в префикс HTTP URL, например: **http://example.com/mylob/businesstaxonomy/task/**;
- **btt:TaskID1** – идентификатор бизнес-задачи. Когда такой идентификатор задачи добавляется к пространству имен **btt**, он может использоваться для получения дополнительных сведений о бизнес-задаче, таких как имя задачи, описание задачи и статистика использования задачи;
- **btt** – пространство имен, которое разрешается в префикс HTTP URL, например: **http://example.com/mylob/businesstaxonomy/task/execution/state**;
- **bttes:200** – код состояния выполнения задачи, указывающий на успешное выполнение задачи;
- **bttes:401** – код состояния выполнения задачи, указывающий на отсутствие разрешения на выполнение задачи.

В силу того что в файлах журнала регистрации содержатся семантические ссылки на бизнес-задачи, выполняющий пересмотр прав доступа получает возможность анализа истории доступа пользователя, а также потенциального доступа пользователя в аспекте выполнения бизнес-задач. После выполнения всестороннего анализа и пересмотра прав доступа пользователя соответствующие обусловленные согласованием изменения направляются обратно Управлению запросами на изменение прав доступа для исправления любых прав доступа пользователя, имеющих избыточные (или недостаточные) привилегии. Эти обусловленные согласованием изменения составляют важный механизм обратной связи, который характеризует любой процесс как жизненный цикл – то есть жизненный цикл процесса IAM. Однако для малых и средних предприятий потребуются не все эти этапы. Например, Организация логики авторизации приложений опускается или реализуется компонентом каталога пользователя. На рисунке I.1 представлены только основные части полного жизненного цикла процесса IAM.

Следующий иерархический маркированный список представляет собой текстовое описание жизненного цикла процесса IAM. Каждый таксономический узел также определен в п. 3.2. Кодифицированное представление см. в модели "Простая система организации знаний" (SKOS) [b-Antonie].

1 Управление бизнес-изменениями

1.1 Организация бизнес-таксономии

1.1.1 Изменение бизнес-процесса

1.1.2 Изменение бизнес-продукта

Дополнение II

Предложение расширения профиля SCIM 2.0

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Следующее расширение профиля – это предлагаемая система для протокола веб-услуг передачи репрезентативного состояния (REST) системы междоменного управления определением идентичности (SCIM) 2.0[1] в качестве основы [b-SCIM REST]. Предлагаемое расширение профиля показано на рисунке II.1. Линии и фигуры черного цвета представляют основные части текущей спецификации SCIM 1.0 [b-IETF SCIM 1.0]. Две фигуры синего цвета ("роли" и "предоставленные права") – это точки расширения SCIM. Сплошные линии и фигуры оранжевого цвета представляют предлагаемые расширения. В силу того что спецификация SCIM оставляет семантический характер "ролей" и "полученных прав" открытым для интерпретации и определения в конкретных реализациях[2], можно далее определить точки расширения, которые станут частью основного стандарта.

Для того чтобы присвоить ролям IAM бизнес-значение, предлагаются следующие рекомендации в качестве расширения профиля текущей спецификации SCIM:

- точка расширения "ролей" SCIM служит контейнером бизнес-ролей, а бизнес-роль состоит из одной или нескольких бизнес-задач;
- точка расширения "предоставленные права" SCIM служит контейнером дополнительных бизнес-задач, которые может выполнять пользователь (в дополнение к тем бизнес-задачам, которые пользователь может выполнять в соответствии с присвоенными ему бизнес-ролями).

---

[1] "Спецификация Системы междоменного управления определением идентичности (SCIM) разработана для упрощения управления определением идентичностей пользователей в приложениях и услугах на базе облака." Из документа: http://www.simplecloud.info/.

[2] SCIM оставляет открытыми для интерпретации и определения в конкретных реализациях следующие понятия:

"**предоставленные права**

Список предоставленных пользователю прав, которые соответствуют тому, что имеет пользователь. То есть предоставленное право – это дополнительное право на предмет, объект или услугу. Какое-либо словарное значение или какой-либо синтаксис не определяются, и, как ожидается, поставщики/потребители услуг закодируют в этом значении достаточную информацию, для того чтобы точно и однозначно определить, к чему именно пользователь имеет доступ. Это значение НЕ ИМЕЕТ каких-либо канонических типов, хотя тип может быть полезен как средство определения области предоставленных прав.

роли

Список ролей пользователя, которые в совокупности определяют, кем является пользователь, например "студент", "преподаватель". Какое-либо словарное значение или какой-либо синтаксис не определяются, однако ожидается, что значение роли представляет собой строку или метку, которой соответствует набор предоставленных прав. Это значение НЕ ИМЕЕТ каких-либо канонических типов". Из документа: https://tools.ietf.org/html/draft-ietf-scim-core-schema-22.

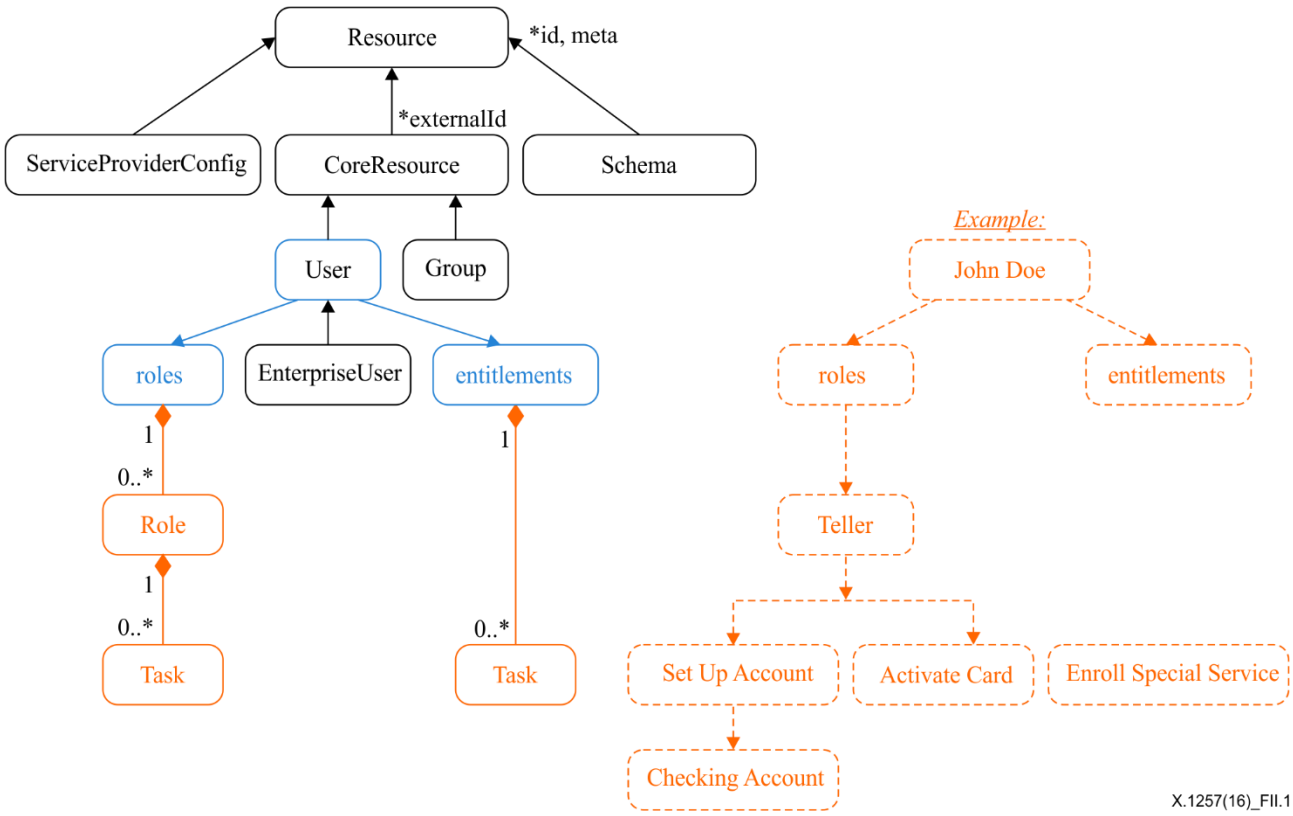

Рисунок II.1 – Расширение профиля SCIM

Пример, выделенный оранжевым цветом, справа, иллюстрирует, что пользователь может иметь бизнес-роль "Банковский служащий", состоящую из двух задач: "Открытие счета" и "Активация карты". Другая задача – "Регистрация особых услуг" – является прямым дополнительно предоставленным правом, для которого пока не требуется создания роли.

Дополнение III

Предлагаемое расширение профиля XACML 3.0

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Для выполнения задачи обеспечения качества данных IAM, описанных в настоящей работе, предлагается следующее расширение профиля.

Предлагается ввести новый тип политики XACML 3.0 [b-OASIS XACML 3.0] – Политику присвоения (обведена красной сплошной линией), анализируемую в ходе обработки запроса на предоставление доступа. Примером служит политика предоставления доступа для обеспечения выполнения правил Разделения обязанностей (SoD) во время предоставления доступа. С другой стороны, Политика доступа (обведена красной пунктирной линией) – это политика, которая анализируется во время выполнения и, как правило, является более сложной (более детальной). На рисунке III.1 показан фрагмент схемы IAM, иллюстрирующий Политику присвоения.

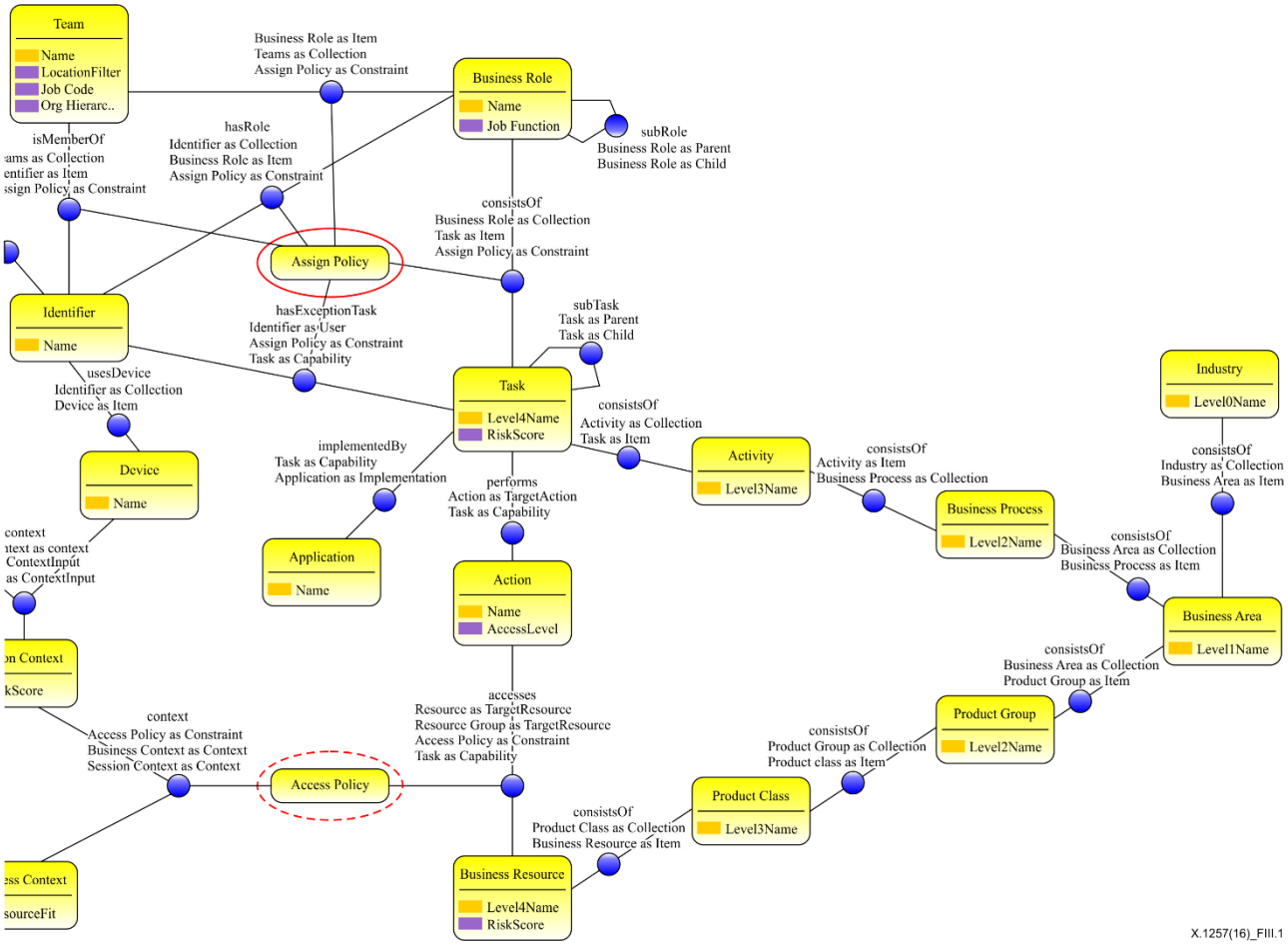

Рисунок III.1 – Фрагмент схемы IAM, иллюстрирующий Политику присвоения

Определим бизнес-семантику модели расширяемого языка разметки контроля доступа (XACML).

a) Ссылка на ресурс осуществляется через идентификацию понятия Бизнес-ресурс. Бизнес-ресурс – это оконечный узел таксономии бизнес-продуктов.

b) Ссылка на действие осуществляется через идентификацию понятий Задача и Действие. Задача – это оконечный узел таксономии бизнес-процессов. Действие – это операция, выполняемая задачей над бизнес-ресурсом.

c) Ссылка на Среду осуществляется через идентификацию понятий Бизнес-контекст и Контекст сеанса. Бизнес-контекст может обеспечить бизнес-атрибуты мелкого уровня, такие как фильтр номеров счетов. Контекст сеанса, имеющий знание о состоянии Аутентификации (регистрационные данные и метаданные устройства), может обеспечить такую информацию, как адрес протокола Интернет (IP) и адрес устройства управления доступом к среде передачи (MAC) для мелкоуровневой технической авторизации.

На рисунке III.2 показано предлагаемое семантическое расширение модели XACML.

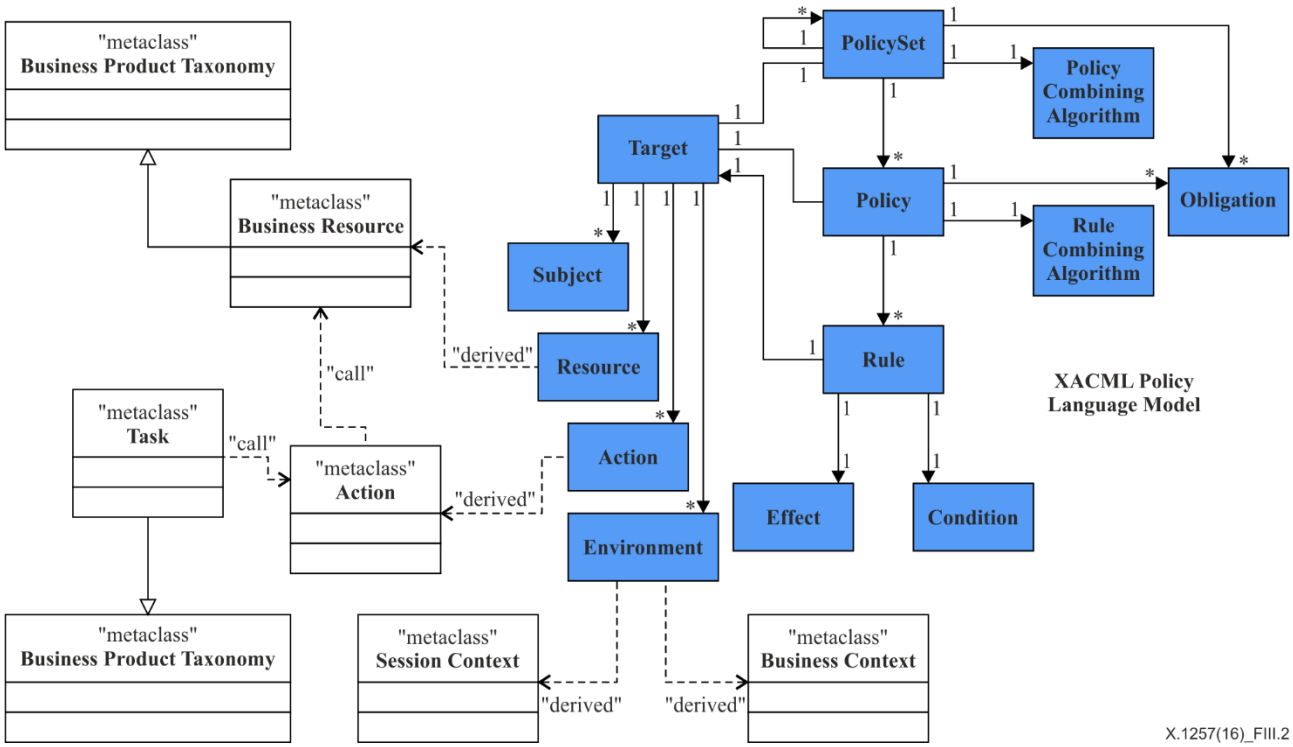

Рисунок III.2 − Предлагаемое семантическое расширении модели XACML

Дополнение IV

Сценарии использования управления доступом на основе задач

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Полезность настоящей Рекомендации иллюстрируют следующие возможные сценарии использования.

1 Политика доступа

a) Пользователю A предоставлено право выполнять бизнес-задачи A, B, C в силу его бизнес-роли A.

b) Пользователю A предоставлено дополнительное право выполнять бизнес-задачу D в силу напрямую предоставленных ему прав.

c) Политика A определяет, что задача B и задача D являются взаимоисключающими для одного и того же номера счета.

d) Для приведенного выше сценария оценивается политика A и выдается решение об отказе.

2 Отчетность о доступе (предоставленные права)

a) Использование понятий задач для улучшения читабельности и понятности описания предоставленных прав на текущем бизнес-языке.

b) Использование понятий бизнес-ресурсов для улучшения читабельности и понятности описания предоставленных прав на текущем бизнес-языке.

3 Использование бизнес-задач

a) Использование существующего справочного веб-приложения, а также:

i) настройки шаблона журнала регистрации приложения для использования идентификаторов бизнес-задач;

ii) создания файлов журнала регистрации во время выполнения приложения.

b) Применение файлов журналов регистрации приложения с аналитическим инструментом:

i) для составления отчета о бизнес-задачах, используемых в производственном цикле;

ii) для обновления бизнес-таксономии на основании вышеупомянутой статистической информации.

4 Использование предоставленных прав

a) Использование существующего справочного веб-приложения, а также:

i) настройки шаблона журнала регистрации приложения для использования идентификаторов бизнес-задач;

ii) создания файлов журнала регистрации во время выполнения приложения.

b) Применение файлов журналов регистрации приложения с аналитическим инструментом:

i) для корреляции событий выполнения бизнес-задач на основе идентификаторов задач;

ii) для корреляции событий отказа в авторизации на основе идентификаторов задач;

iii) для составления аналитических отчетов с указанием противоречивых сценариев SoD за прошедшее время.

Дополнение V

Возможные механизмы реализации интерфейса бизнес-таксономии

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Решения на основе стандартов, таких как нормализованная лексика SKOS[3] [b-Antonie] или механизм реестра метаданных, могут обеспечить идентификацию и регистрацию понятий бизнес-таксономии. Система SKOS особенно полезна для представления иерархических отношений.

Другим возможным решением является использование сериализации связанных данных на основе нотации объектов JavaScript (JSON) (JSON-LD) [b-W3C JSON-LD], называемой также JSON-Linked Data. При том что JSON-LD позволяет смешивать различные нормализованные лексики и может представлять сложные графические отношения, стандарта интерфейса таксономии не существует. На данный момент не существует ни реализаций REST, ни реализаций простого протокола доступа к объектам (SOAP).

[3] SKOS обеспечивает базовые иерархические отношения, такие как расширение и сужение, однако не допускает более конкретных онтологических отношений, которые могут потребоваться для выражения синтаксиса и значения элементов данных IAM.

Дополнение VI

Стандарты таксономии бизнес-процессов

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

В настоящей Рекомендации упоминается не менее двух типов бизнес-таксономии – таксономия бизнес-процессов и таксономия бизнес-продуктов. Эти термины введены органами по стандартизации управления бизнес-процессами, например в таких документах, как Расширенная карта бизнес-процессов оператора электросвязи, разработанная TeleManagement Forum (eTOM), и Классификации основных продуктов (CPC) [b-CPC].

В примере, представленном на рисунке VI.1, показана структура классификации процессов (PCF) Американского центра проблем повышения производительности и качества продукции (APQC) [B-APQC-PCF], а также показано, как могут быть классифицированы процессы.

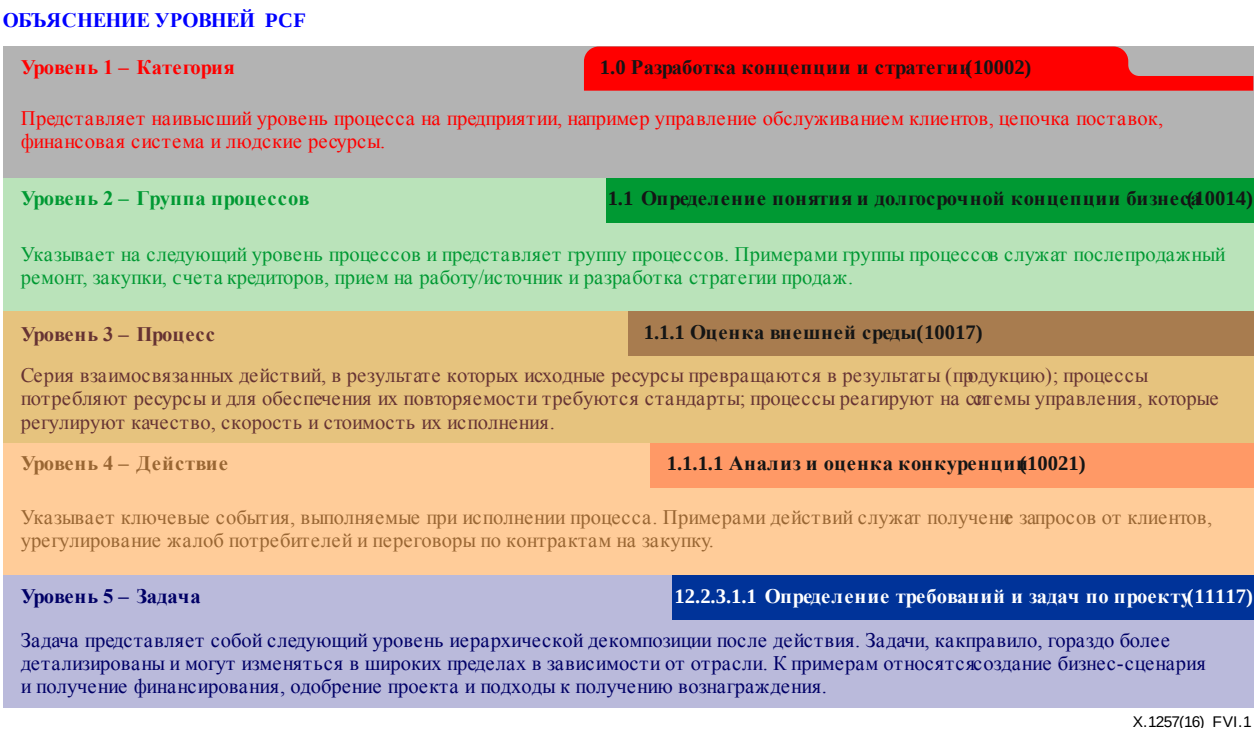

Рисунок VI.1 − Определения структуры таксономии бизнес-процессов

Дополнение VII

Онтологическая модель домена IAM

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Полная онтологическая модель домена IAM изображена на рисунке VII.5. Для того чтобы читателю было проще понять домен IAM, прежде представлены следующие предметные области IAM:

- рисунок VII.1 – модель домена IAM – предметная область Пользователь;
- рисунок VII.2 – модель домена IAM – предметная область Предоставление доступа;
- рисунок VII.3 – модель домена IAM – предметная область Контроль доступа;
- рисунок VII.4 – модель домена IAM – предметная область Бизнес-домен.

В итоге указанные выше предметные области объединяются в полную модель домена IAM, показанную на рисунке VII.5. Первая предметная область относится к типам понятия "пользователь". Согласно [ITU-T X.1252] и X.1254 [ITU-T X.1254] пользователь представлен Объектом в нескольких аспектах, таких как суть или существование субъекта. Объект имеет одну или несколько Идентичностей. Идентичность имеет один или несколько Идентификаторов.

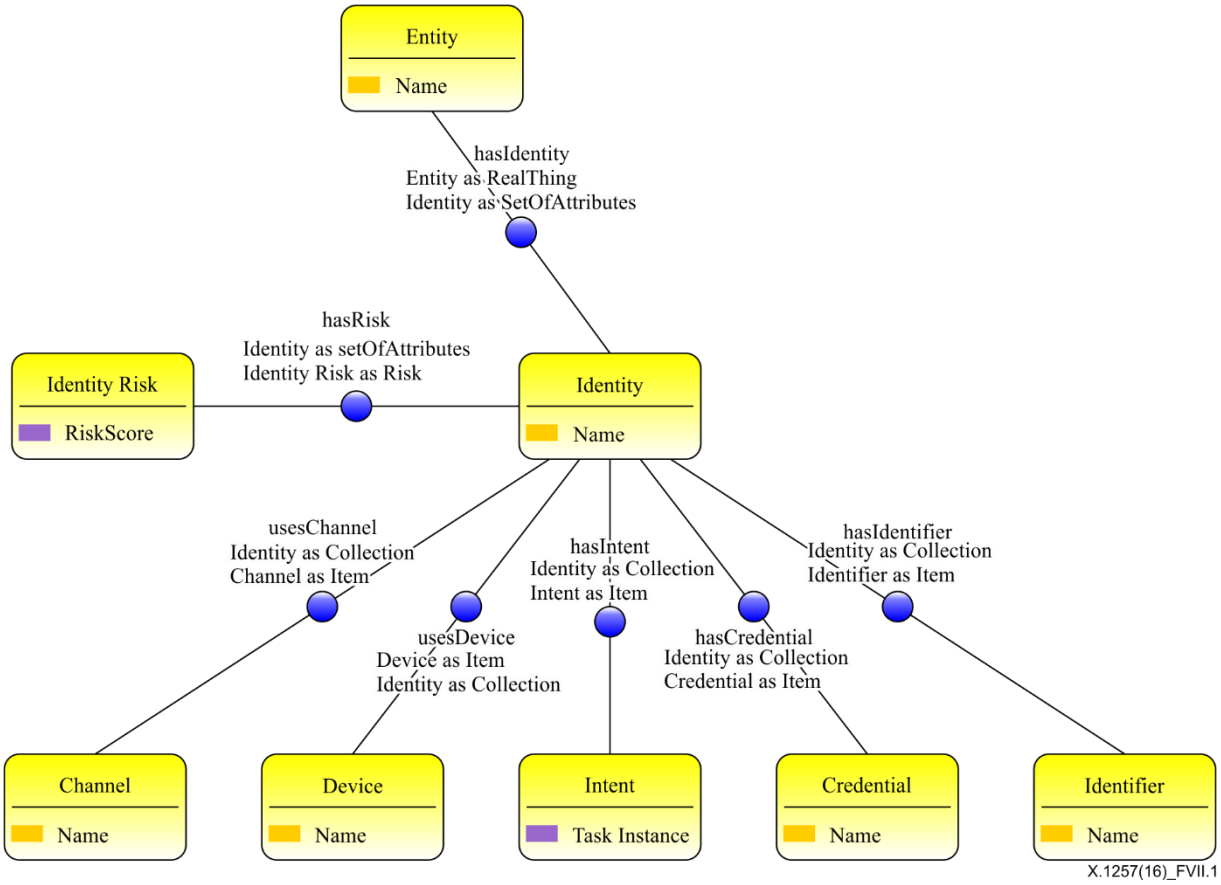

Рисунок VII.1 − Модель домена IAM – предметная область Пользователь

Пример: человек – живое существо – является Объектом, который характеризуется именем, датой рождения и т. д. Этот человек может быть одновременно работником и клиентом и, следовательно, может иметь не менее двух идентичностей. Впоследствии работник получит идентификатор EmployeeID, а клиент получит идентификатор CustomerID.

ПРИМЕЧАНИЕ. − В некоторых случаях роль человека может играть устройство, которое действует от имени человека.

На рисунке VII.2 иллюстрируется предметная область Предоставление доступа. Предоставление доступа заключается в присвоении пользователю прав доступа через его идентификатор(ы). Права доступа могут присваиваться пользователю в рамках Группы (Групп), членом которой(ых) он/она является. Группа в данном контексте – это блок прав доступа, обусловленных людскими ресурсами. В дополнение к правам доступа как члена группы пользователь может получить права доступа через бизнес-роль, которую он/она может выполнять. Наконец, в порядке исключения, пользователю может быть предоставлено право выполнения определенных бизнес-задач. В конечном итоге права доступа – это набор задач, которые может выполнять пользователь. Однако все назначение задач пользователям оценивается на основании определенных применимых предоставленных прав, называемых "Политика присвоения", которая исключает деструктивные сочетания предоставленных прав, а также обеспечивает выполнение правил Разделения обязанностей (SoD).

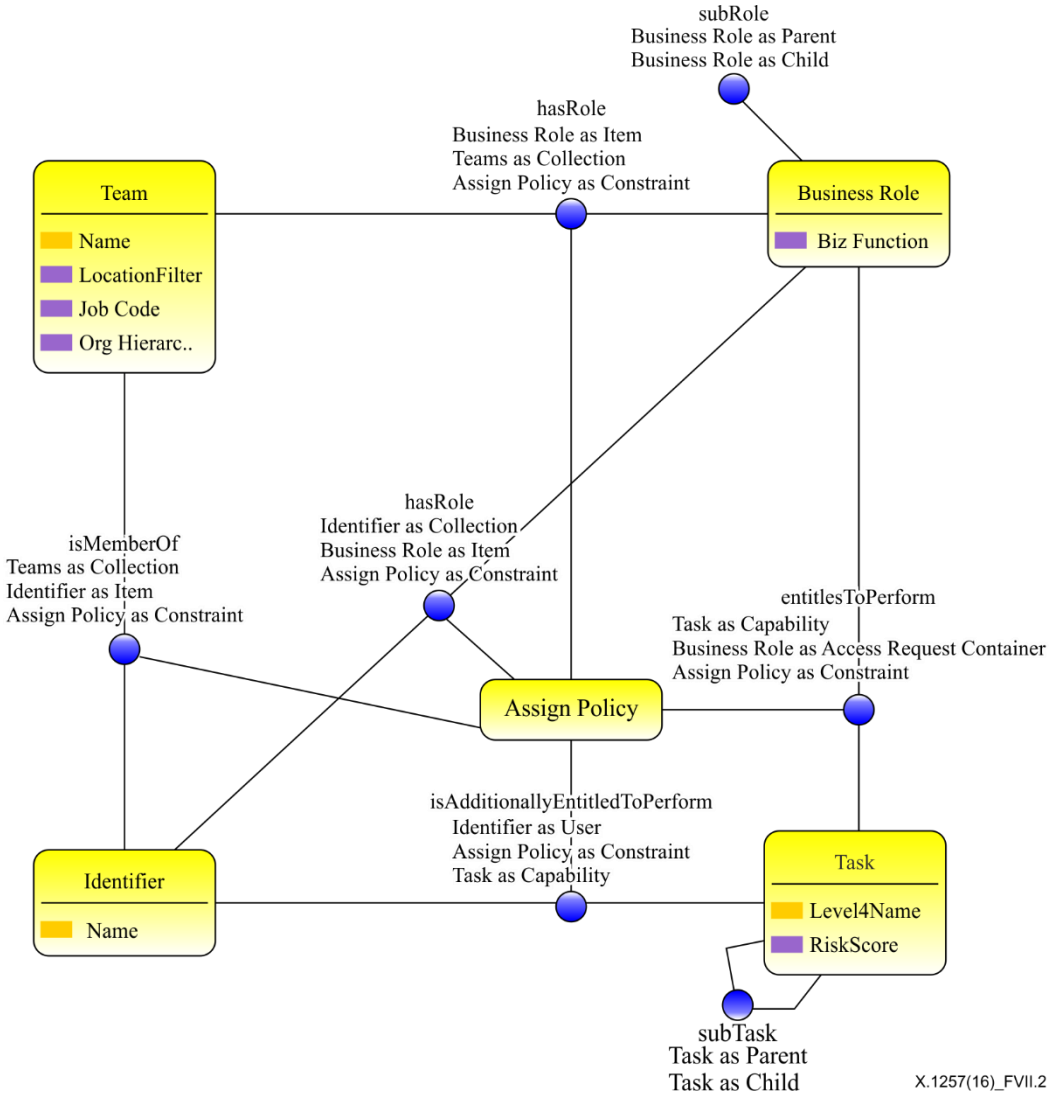

Рисунок VII.2 − Модель домена IAM – предметная область Предоставление доступа

Пример: пользователь A является членом группы X. Каждый член группы X, который находится в месте расположения штаб-квартиры (т. е. Регион=основной, Подразделение=основное), имеет пять бизнес-ролей, и каждая бизнес-роль предоставляет пользователю право выполнять 10 задач. Таким образом, по умолчанию любой член группы X может выполнять 50 задач. Кроме того, пользователю A назначены еще три бизнес-роли, которые предоставляют этому пользователю право выполнять еще 5 задач. Пользователю A предоставлено также право выполнения еще одной задачи напрямую в порядке исключения. В итоге пользователю A предоставлено право выполнять 66 отдельных задач. Однако те члены группы, которые не находятся в штаб-квартире, будут иметь всего по три бизнес-роли – то есть на 30 бизнес-задач меньше.

Следующая предметная область – Контроль доступа – охватывает выполнение авторизации на основе политики и задач в зависимости от предоставленных пользователю прав и контекста сеанса. Конкретная задача осуществляет доступ к определенному(ым) ресурсу(ам), если соответствующая Политика доступа позволяет осуществить этот доступ. Политика доступа анализирует свои правила на основании Контекста сеанса и Ограничений доступа соответствующего пользователя. Контекст сеанса содержит метаданные аутентификации пользователя, такие как Канал, Устройство, Намерение, Регистрационные данные и Идентификатор.

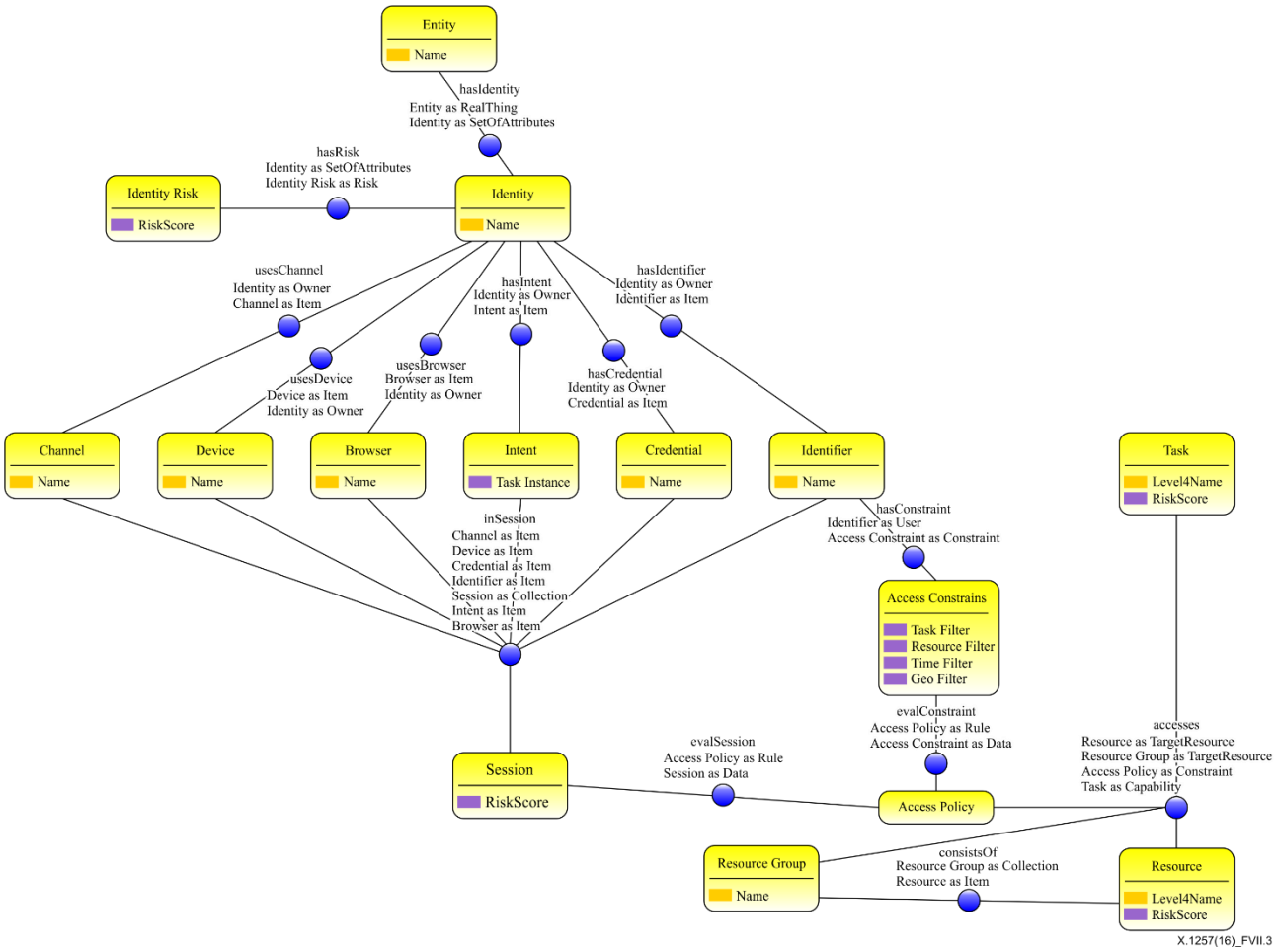

Рисунок VII.3 − Модель домена IAM – предметная область Контроль доступа

Пример: пользователь A намеревается выполнить задачу "Открытие счета". Эта задача будет осуществлять доступ к бизнес-ресурсу (т. е. его создание) "Расширенный текущий счет". Такой доступ осуществляется, если оценка соответствующей политики доступа дает положительный результат. Политика доступа гарантирует, что определенный пользователь должен использовать для этой транзакции надлежащий Канал и что IP-адреса находятся в пределах допустимого диапазона IP-адресов. В этот момент времени политика может также обращаться к временному хранилищу неразрешенных задач, поскольку это прошлое рабочее время.

Последняя предметная область – бизнес-таксономия – иллюстрирует взаимодействие домена IAM и бизнес-домена. Бизнес-таксономию составляют бизнес-процессы и бизнес-продукты. Как видно на рисунке (справа налево), первые два уровня этой таксономии – Отрасль и Бизнес-область. Слева от Бизнес-области находятся две иерархические структуры – таксономия бизнес-процессов и таксономия бизнес-продуктов. Как правило, Задача является оконечным узлом в таксономии бизнес-процессов, а бизнес-ресурс – оконечным узлом в таксономии бизнес-продуктов. Приложение – это реализация соответствующих задач, и оно выполняет доступ к ресурсам от имени пользователя.

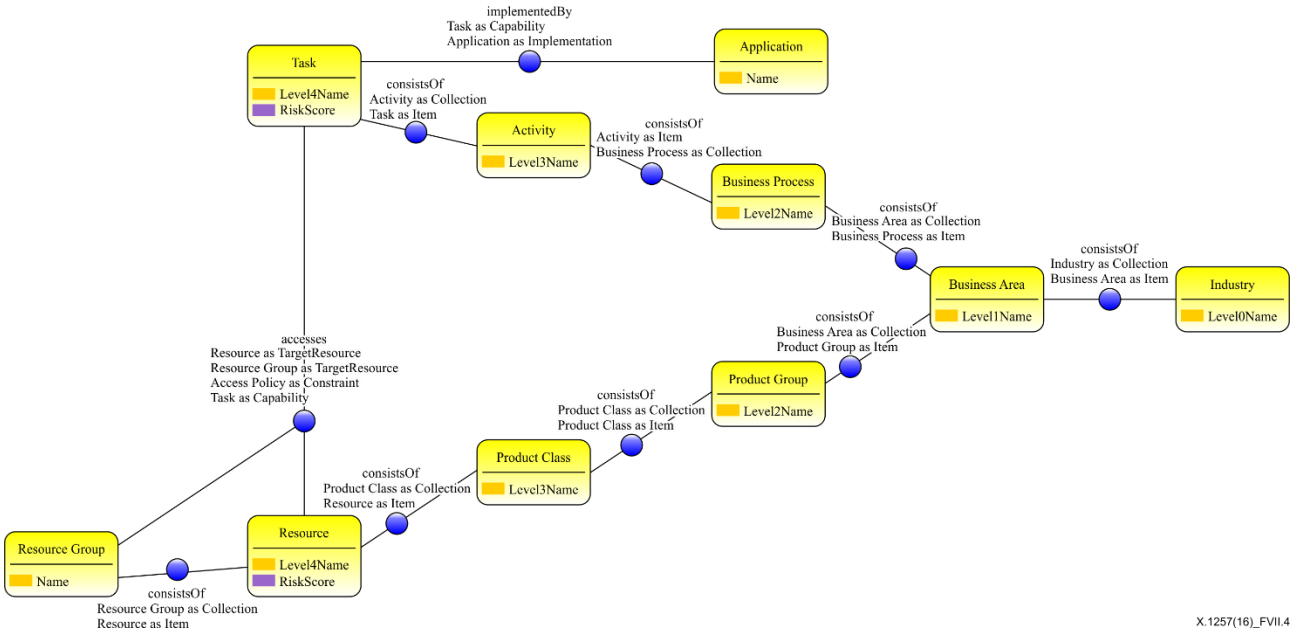

Рисунок VII.4 − Модель домена IAM – предметная область Бизнес-домен

Пример: Отрасль – финансовая; Бизнес-область – обслуживание клиентов; Бизнес-процесс – Создание; Действие – Работа со счетом; Задача – "Открытие счета". В аспекте таксономии бизнес-продуктов: Группа продуктов – Расчетный счет, Класс продуктов – Текущий счет, и Бизнес-ресурс – "Расширенный текущий счет".

Наконец, полная модель домена IAM представлена на рисунке VII.5, ниже, где соединены все четыре предметные области, упомянутые выше.

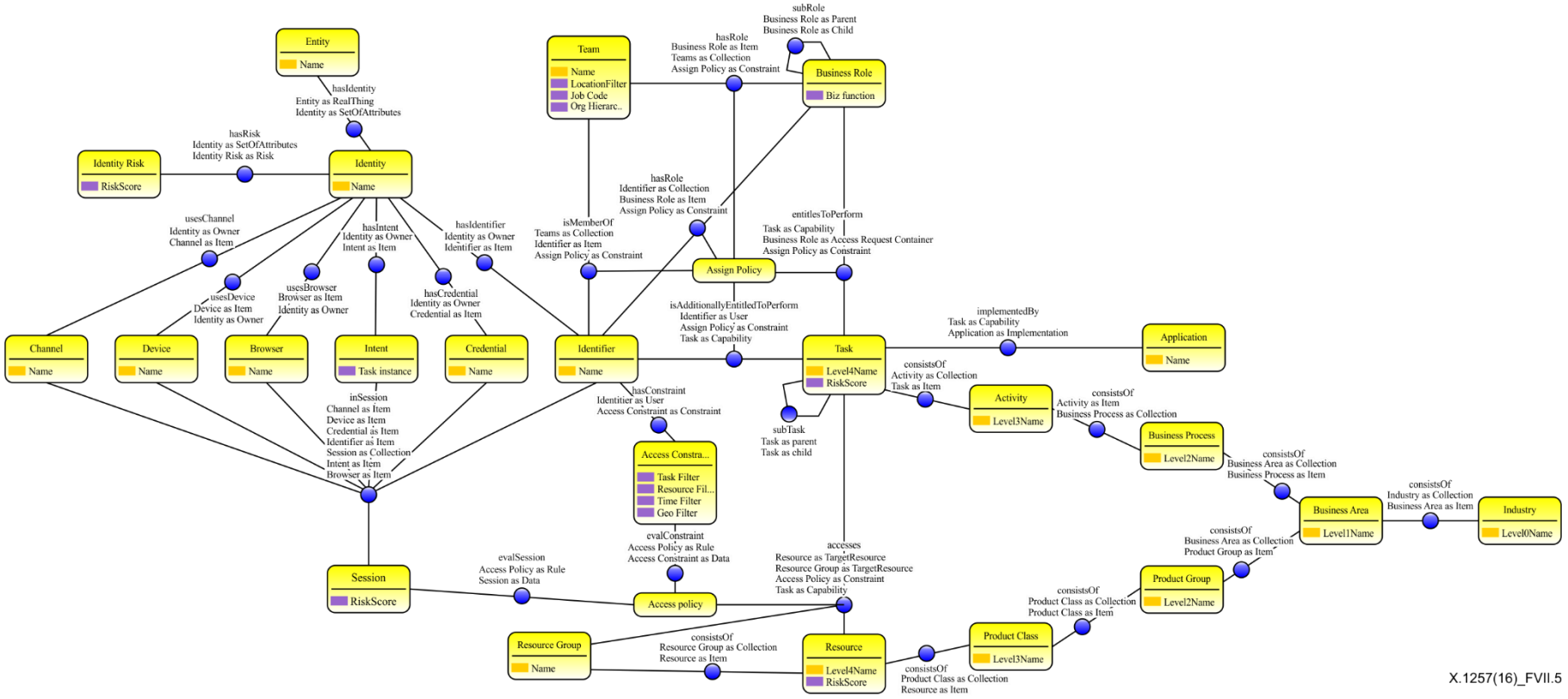

Рисунок VII.5 – Модель домена IAM

Показанная на рисунке VII.5 модель домена моделирует отношения между понятиями в соответствии с требованиями, установленными в соответствующем разделе. Эта схема представляет следующие ниже основные принципы.

- Пользователь представлен его Объектом, Идентичностями, Идентификаторами и другими характеристиками. В процессе Присвоения предоставленных прав пользователю может быть предоставлено право выполнения конкретных задач через Группу и роль (обычно в 80% случаев) или непосредственно назначено выполнение конкретных задач (в порядке исключения в 20% случаев).
- Группа – это блок ролей людских ресурсов. Основное назначение типов Группа и Бизнес-роль заключается в ускорении и упрощении процесса Присвоения и Утверждения предоставленных прав.
- Бизнес-роли должны наследовать бизнес-значение от соответствующих бизнес-задач.

ПРИМЕЧАНИЕ. − В настоящее время роли IAM создаются и сопровождаются структурами ИТ и, следовательно, не имеют прямо прослеживаемого бизнес-значения. Во многих случаях для успешного пересмотра прав доступа недостаточно опираться только на название роли для передачи бизнес-значения.

- Задачи – это оконечные узлы таксономии бизнес-процессов, создаваемые и сопровождаемые бизнес-архитекторами и специалистами по бизнес-моделированию.
  - Задачи, как правило, более детализированы по сравнению с приложениями, которые их реализуют.
  - Задачи реализуются соответствующими приложениями.
  - Задачи представляют Обязанности как в сценариях Разделения обязанностей (SoD).

ПРИМЕЧАНИЕ. − SoD невозможно осуществить без соответствующих бизнес-задач.

- Пользователь не имеет прямого доступа к Бизнес-ресурсу. Вместо этого пользователю предоставлено право выполнять Бизнес-задачу, а Бизнес-задача осуществляет доступ к Бизнес-ресурсу(ам) от имени пользователя.
- Процесс-Действие-Задача – это логическая структура и часть таксономии бизнес-процессов для определения и организации бизнес-процессов стандартным образом [b-APQC PCF 5.0.1] и, как правило, она сопровождается бизнес-архитекторами и специалистами по моделированию бизнес-процессов.
- Группа продуктов – Класс продуктов – Бизнес-ресурс – это логическая структура и часть таксономии бизнес-продуктов для определения и организации бизнес-процессов стандартным образом [b-CPC Ver 2] и, как правило, она сопровождается бизнес-архитекторами и специалистами по моделированию бизнес-процессов.
- Политика присвоения – это ограничительный механизм присвоения предоставленных прав, который применяется на этапе Присвоения предоставленных прав для предотвращения злоупотреблений и деструктивных статических сочетаний бизнес-задач.
- Политика доступа – это ограничительный механизм Осуществления доступа, который применяется на этапе Рабочего цикла Доступа для предотвращения злоупотреблений и деструктивных динамических сочетаний времени выполнения.
- Бизнес-ресурсы – это понятия, такие как история болезни, ссудный счет или текущий счет. Они позволяют осуществлять присвоение предоставленных прав и контроль доступа на уровне ресурсов с мелкой разбивкой.
- Предоставленные бизнес-права – это задача(и), выполнять которую(ые) пользователю предоставлено право (т. е. предоставленные бизнес-права с крупной разбивкой).
- Бизнес-разрешения – это задача(и), которая(ые) осуществляет(ют) доступ к конкретным бизнес-ресурсам и ограничена(ы) политикой.
- При выделении предоставленных прав пользователю предоставленные бизнес-права при необходимости могут быть преобразованы в соответствующие системные разрешения.
- Системные разрешения относятся к системным ресурсам, таким как базы данных, таблицы, столбцы, файлы или наборы данных мейнфрейма.

Библиография

[b-ITU-T X.1255] Рекомендация МСЭ-Т X.1255 (2013 г.), Структура обнаружения информации по управлению определением идентичности.

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2011, *Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts.*

[b-Antonie] Antoine Isaac, E.S. (2009, August 18), *SKOS simple knowledge organization system primer*.
http://www.w3.org/TR/skos-primer/ (По состоянию на 18 мая 2016 г.)

[b-APQC-PCF] Tesmer, John (2014, March), *Process Classification Framework 6.1.1*.
http://www.apqc.org/process-classification-framework (По состоянию на 18 мая 2016 г.)

[b-APQC PCF 5.0.1] APQC PCF. (2011, June), *Banking Process Classification Framework*.
http://www.apqc.org/knowledge-base/download/33193/PCF_Banking_Ver_5.0.1_2011.pdf
(По состоянию на 18 мая 2016 г.)

[b-CPC] http://en.wikipedia.org/wiki/Central_Product_Classification

[b-CPC Ver 2] CPC Workgroup. (2008, December 31), *Central Product Classification, Ver.2, Detailed structure and explanatory notes*.
http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=25 (По состоянию на 18 мая 2016 г.)

[b-example] http://www.apqc.org/knowledge-base/documents/apqc-process-classification-framework-pcf-banking-excel-version-501

[b-IETF SCIM 1.0] C. Mortimore, Ed. (2013, April 15), *System for Cross-Domain Identity Management: Core Schema*.
http://tools.ietf.org/html/draft-ietf-scim-core-schema-01 (По состоянию на 18 мая 2016 г.)

[b-IETF SCIM 2.0] Hunt, e.a. (2015, June 8), *System for Cross-Domain Identity Management: Core Schema*.
https://tools.ietf.org/html/draft-ietf-scim-core-schema-22 (По состоянию на 18 мая 2016 г.)

[b-NIST-RBAC 2000] Sandhu, R., David, F., & Khun, R. (2000), *The NIST Model for Role-Based Access Control: Towards A Unified Standard*.

[b-OASIS XACML 3.0] Erik Rissanen. (2013, January 22), *eXtensible Access Control Markup Language (XACML) Version 3.0*.
http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
(По состоянию на 18 мая 2016 г.)

[b-OBAC] Mohammad, A. (2011, March 7), *Ontology-Based Access Control Model for Semantic Web*.
http://www.worldacademicunion.com/journal/1746-7659JIC/jicvol6no3paper03.pdf
(По состоянию на 18 мая 2016 г.)

[b-schema.org 2011] Google, Yahoo, Bing, Yandex. (2011), *schema.org*.
http://schema.org (По состоянию на 18 мая 2016 г.)

[b-SCIM REST] SCIM 2.0 REST web service protocol, C. Mortimore, Ed., 2013.
http://www.simplecloud.info/ (По состоянию на 18 мая 2016 г.)

[b-W3C JSON-LD] Manu Sporny. (2013, August 6), *JSON-LD 1.0, A JSON-based* Serialization *for Linked Data*.
http://json-ld.org/spec/latest/json-ld/ (По состоянию на 18 мая 2016 г.)

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2016 г.