УДК: 004.056.53

С.Н. Чуруброва

ОБОСНОВАНИЕ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ В СИСТЕМАХ ПОДДЕРЖКИ ОРГАНИЗАЦИОННЫХ РЕШЕНИЙ

В статье рассматриваются доминирующие модели управления доступом – DAC, MAC, RBAC и относительно новая - ABAC. Цель выбрать модель обладающую свойствами абстрактности, простоты и адекватности системам поддержки принятия решений. Каждая модель имеет свои преимущества и недостатки, но важно отметить эволюцию этих моделей, чтобы полностью оценить гибкость и применимость модели ABAC в системах поддержки принятия решений.

Ключевые слова: система поддержки принятия решений, модель управления доступом, ABAC.

Введение

В настоящее время, в связи с ускоренными темпами информатизации общества и глобальным ростом объемов хранения цифровых данных все более остро встают вопросы защиты информации. Один из основных способов уменьшения информационного риска состоит в правильном распределении полномочий. Данный механизм в информационных системах представлен в виде подсистемы управления и контроля доступа, реализующей модель управления доступом [1].

Повышение сложности организационных структур и бизнес-процесов ставит новые задачи для подсистем доступа к данным. Интересы владельцев информации заключаются в том, чтобы определенная информация — конфиденциальная коммерческая, персональная информация и т.д., была бы постоянно легко доступна и в то же время надежно защищена от неправомерного ее использования. Кроме того, распределение функций между сотрудниками предполагает предоставление каждому из них соответствующих ресурсов, причем различным типам пользователей в различных процессах необходим доступ к различным типам данных.

Исследования в области разграничения и управления доступом в основном сосредоточены на расширении доминирующих моделей управления доступом, разработке моделей управления доступом для веб-сервисов, распределенных информационных систем. Но нет исследований по разработке модели управления доступом в системах поддержки принятия решений (СППР) с учетом современных особенностей развития данных систем и характеристик, которые являются критическими для выработки качественного решения.

Сегодня лица принимающие решения сталкиваются с большим объемом разнообразных, с потенциально высокой изменчивостью данных, требующих проверки и оценивания, более того — поступающих с огромной скоростью. Исследования в СППР показывают, что лица, принимающие решения могут работать более оперативно, используя данные в режиме реального времени, более точно из-за интеллектуального анализа данных и методов "Больших данных" (Big data), более стратегически с учетом большего числа факторов [2]. Однако «Большие» вовсе не обязательно значит «необходимые» или «лучшие» данные. Самое сложное в Больших данных это управление ними. Без должной организации доступа к данным создается не только угроза информационной безопасности, но также риск снижения качества решений.

Объект исследования: модели управления доступом.

Цель исследования: выбор оптимальной базовой модели для разработки подсистемы управления доступом в современных СППР, с учетом всех особенностей функционирования данных систем.

Методы управления доступом

Управление доступом является одной из приоритетных задач в области информационной безопасности. Механизм управления доступом может быть определен как логический компонент, который служит для получения запроса на доступ от субъекта, чтобы решить и исполнить решение доступа [3].

Цель логического контроля доступа — защитить данные от несанкционированных операций доступа. Управление доступом позволяет защитить важные данные и в то же время не препятствовать их совместному использованию сотрудниками организации. Объекты доступа принадлежат лицам или организациям и имеют некоторое присущее им значение, которое мотивирует владельцев защищать их. Как владельцы объектов, они имеют право устанавливать политику, которая описывает, какие операции могут быть выполнены над объектами, кем, и в каком контексте эти субъекты могут выполнять эти операции. Если субъект удовлетворяет политике управления доступом, установленной владельцем объекта, то субъект авторизован для выполнения требуемой операции на этот объект – т.е. ему предоставлен доступ к объекту. Если субъект не удовлетворяет требованиям политики, то доступ к объекту запрещен.

Эти функции механизма управления доступом могут быть описаны в терминах различных логических моделей управления доступом.

Модели управления доступом

Модель управления доступом играет основную роль в комплексной системе защиты информации. Цель модели – выражение сути требований по безопасности к данной системе [4]. Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информации.

Модели управления доступом обеспечивают основу и набор граничных условий, на которых объекты, субъекты, операции и правила могут быть объединены, чтобы генерировать и приводить в исполнение решения механизма управления доступом [3].

Базовые понятия модели управления доступом:

–*Доступ к информации* — возможность получения информации, ее использования и обработки;

–*Правила разграничения доступа* — совокупность правил, регламентирующих права (политики) доступа субъектов доступа к объектам доступа;

–*Объект доступа (пассивные объекты)* — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа;

–*Субъект доступа (активные объекты)* — лицо или процесс, действия которого регламентируются правилами разграничения доступа;

–*Атрибуты доступа* — любая информация, которая используется при управлении доступом и связана с субъектами, объектами или процессами.

Эволюция управления доступом

До 1985 года цифровые данные составляли менее процента от всей информации. После 2007 – около 94% [5]. После 2000 года отмечается глобальный рост объемов хранения данных по сравнению с предыдущим периодом, что отразилось на эволюции моделей управления доступом.

До 1992 года существовали две основные модели управления доступом: модель мандатного (принудительного) управления доступом (MAC, mandatory access control) и модель дискретного (избирательного) управления доступом (DAC, discretionary access control). Данные модели были приняты в качестве стандарта Министерством обороны США. Модель MAC нашла применение в основном для контроля доступа в многоуровневых военных информационных системах, а DAC – во многих коммерческих операционных системах, включая Windows.

Дискреционные модели управления доступом – модели, в которых владелец ресурса сам задает права доступа к нему. В большинстве случаев права доступа субъектов к объектам представляются в виде матрицы или списков доступа [6]. К достоинствам дискретной политики безопасности можно отнести относительно простую реализацию соответствующих механизмов защиты. При запросе доступа к объекту, система ищет субъекта в списке прав доступа объекта и разрешает доступ, если субъект присутствует в списке и разрешенный тип

доступа включает требуемый тип. Иначе доступ не предоставляется. Недостатком модели DAC является то, что каждый объект должен иметь владельца, который может делать с ним все, что угодно, а также передать право на чтение другим субъектам. В DAC, информация может быть доступна для не авторизованных пользователей, потому что нет контроля для копий объектов. Кроме того модель не контролирует потоки информации и может быть уязвима для атак «троянским конем». Динамичность современной программной среды в сочетании со сложностью отдельных компонентов существенно сужает область применимости дискреционной модели управления доступом. При определении допустимости доступа важно не только (и не столько) то, кто обратился к объекту, но и то, какова семантика действия.

В *мандатной модели управления доступом* режим доступа субъектов к объектам определяется установленным режимом конфиденциальности [6]. В отличие от дискретной политики, которая требует определения прав доступа для каждой пары субъект-объект, мандатная политика, назначением метки секретности объекту, однозначно определяет круг субъектов, имеющих права доступа к нему. И. наоборот, назначением метки секретности субъекту, однозначно определяется круг объектов, к которым он имеет права доступа. MAC имеет дело с потоком информации и накладывает ограничение на передачу информации от одного пользователя другому, что решает проблему троянских коней. Общее правило звучит так: *пользователи могут читать только документы, уровень секретности которых не превышает их допуска, и не могут создавать документы ниже уровня своего допуска.* То есть теоретически пользователи могут создавать документы, прочесть которые они не имеют права.

Модель полностью формализована математически. До сих пор в измененном виде применяется в военной отрасли. Основной упор в модели делается на конфиденциальность, но кроме неё фактически больше ничего не представлено. Кроме того, в модели игнорируется проблема изменения классификации: предполагается, что все сведения относятся к соответствующему уровню секретности, который остается неизменным. В данной модели есть только два права доступа – чтение и запись, которых явно недостаточно для моделирования сложных процессов.

Ролевая модель (RBAC, Role-Based Access Control), разработанная в 1992 году [7], послужила новым витком эволюции моделей управления доступом и сейчас является одной из самых используемых моделей.

Ролевая модель управления доступом, копируют иерархическую структуру организации, что позволяет упростить администрирование [6]. Модель RBAC контролирует доступ пользователей к информации на основе типов их активностей в системе (ролей). Роли позволяют получить конкретным лицам доступ к ресурсам в той степени, в какой это необходимо им для выполнения своих обязанностей.

Управление доступом при использовании ролевой модели осуществляется следующим образом: 1) Для каждой роли указывается набор полномочий, представляющий собой набор прав доступа к объектам АС. 2) Каждому пользователю назначается список доступных ему ролей. Отметим, что пользователь может быть ассоциирован с несколькими ролями.

Основным достоинством ролевой модели является близость к реальной жизни. Роли, действующие в АС, могут быть выстроены в полном соответствии с корпоративной иерархией и при этом привязаны не к конкретным пользователям, а к должностям. С помощью RBAC могут быть смоделированы дискреционные и мандатные системы управления доступом, а так же реализовано динамичное управление доступом, но с определенными ограничениями. Главной проблемой модели является т.н. «Ролевой взрыв» – трудности масштабирования RBAC для удовлетворения сложных требований управления доступом. Он обусловлен ситуацией, когда каждая роль требует различных наборов разрешений и должна быть определена большим количеством функций. По данным исследования [8] количество ролей в среднем в 1,5 раза превышает количество

пользователей системы. Еще одно препятствие перед использованием ролевой модели в ряде систем – это отсутствие в ней понятия владельца объекта. Другими словами, пользователь, создавший объект, не имеет на него никаких исключительных прав. Зачастую эту задачу решают, используя внешние по отношению к модели средства (например, вводят в ролевую модель элементы дискреционной или атрибутивной), и, соответственно, не снимают ограничений самой модели.

Для учета различных особенностей современных информационных систем предложено множество модификаций RBAC. Однако растущее недовольство ограничениями ролевой модели, которые в ряде случаев сильно затрудняют ее использование, вызвало новые направления исследований — с одной стороны исследователи старательно и творчески расширяют модель RBAC, другие развивают новую логическую модель управления доступом на основе атрибутов (ABAC, Attribute Based Access Control) [9].

Модель управления доступом на основе атрибутов

Атрибутная модель управления доступом является наиболее универсальной [6]. Основная идея данной модели заключается в том, что решение о предоставлении доступа субъекта к объекту принимается на основе анализа набора произвольных атрибутов, связанных с субъектом, объектом или даже средой их функционирования. Модель ABAC призвана преодолеть ограничения доминирующих моделей доступа (DAC, MAC и RBAC), одновременно объединив их преимущества [10].

ABAC — метод контроля доступа, где субъекту, который делает запрос на выполнение операции над объектом, предоставляется или отказывается в доступе на основе присвоенных атрибутов субъекта, присвоенных атрибутов объекта, средой их функционирования (контекст) и набора политик, определяющих допустимые операции для субъект-объектных комбинаций атрибутов. Данное определение ABAC изображено на рисунке (рис.1), где механизм контроля доступа, получая запрос на доступ от субъекта, проверяет: а- правила; атрибуты субъекта; в- атрибуты объекта; г- среды функционирования (контекст) для определения авторизации (права) объекта на запрашиваемые действия. Субъект получает доступ к объекту, если авторизован.

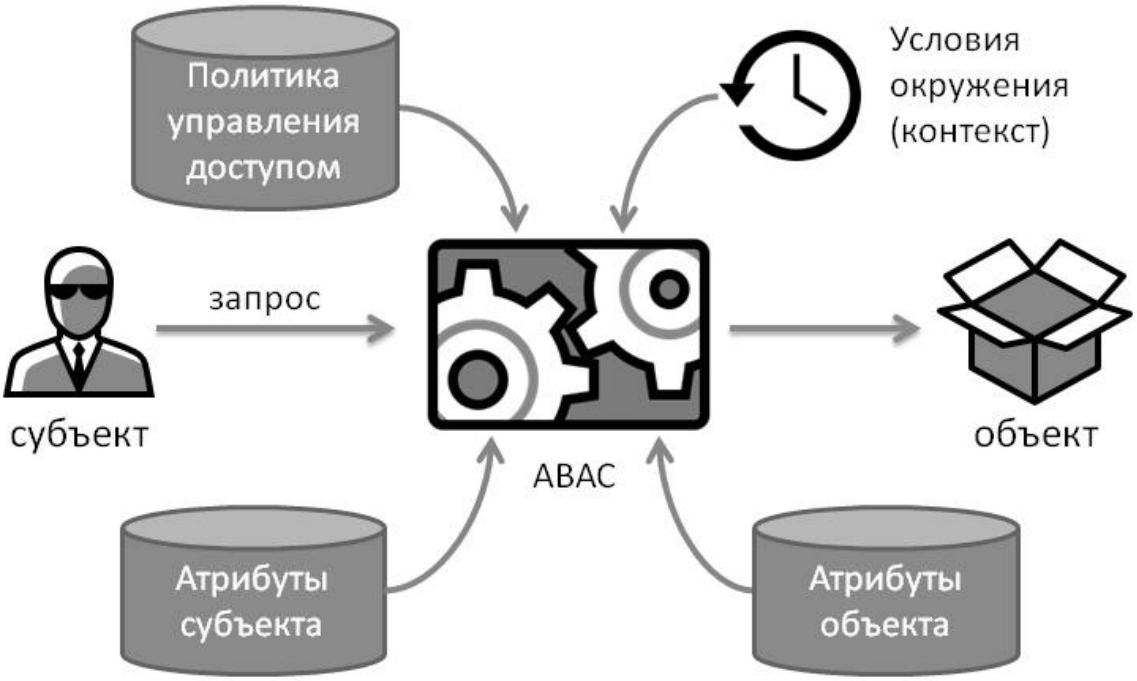

Рис.1. Базовый сценарий контроля доступа в ABAC.

Базовые понятия ABAC [3]:

Атрибуты — это характеристики субъекта, объекта или условий выполнения операции. Атрибуты содержат информацию, представленную парой имя-значение.

Субъект — это пользователь (человек) или Non-Person Entity, например процесс или устройство, что выдает запросы на выполнение операций над объектами. С субъектами связан один или больше атрибутов.

Объект — единица информационного ресурса АС, доступ к которой контролируется ABAC системой. Это может быть любой объект запроса, над которым возможно выполнение операции субъекта, включая данные, приложения, сервисы, устройства и сети или области хранящие информацию.

Операция — это выполнение функции запроса субъекта над объектом. Операции включают чтение, запись, редактирование, удаление, копирование, выполнение и модификацию.

Политика — это представление правил или отношений, которые позволяют определить, может ли запрос доступа быть удовлетворен, учитывая значения атрибутов субъекта, объекта и, возможно, среды функционирования.

Среда функционирования (Environment conditions) — оперативный или ситуативный контекст, в котором происходят запросы доступа. Среда функционирования проявляется в характеристиках окружения. Характеристики окружения не зависят от субъекта или объекта, это могут быть: текущее время, день недели, местоположение пользователя, или текущий уровень угрозы.

В отличие от моделей основанных на идентификации, ABAC — это не вопрос «кто?», а вопросы «что?», «где?», «когда?», «почему?» и «как?».

Особенностью модели является многомерность бизнес-правил, которые она способна поддерживать. Пример одномерного бизнес-правила: «Только администратор может управлять системой» или «Только бухгалтер может заниматься финансовой деятельностью» — все действия можно разбить по ролям (бухгалтер, администратор и т. п.), тогда ролевого подхода будет достаточно — одному бизнес-правилу будет соответствовать одна роль. Но бизнес-правила неизбежно усложняются и становятся многомерными. Это приводит к тому, что одного атрибута (роли) для выражения бизнес-правил становится недостаточно и начинают добавляться другие атрибуты (город, страна, филиал, день недели, владелец, лимит и т. п.). – ABAC позволяет учитывать все атрибуты, при этом многомерные правила не становятся сложными. Нужно лишь добавить логическое условие к политике. При добавлении новых значений атрибутов правила меняться не будут. Таким образом, ABAC позволяет избежать проблем, которые появляются в RBAC: бизнес-правило не «размазывается» по системе, что делает его понимание и поддержку достаточно простыми; не происходит взрывного роста числа условий, что упрощает их сопровождение.

ABAC предприятия

Базовая архитектура механизма ABAC включает в себя такие две основные функции, как точка принятия решения на основе заданной политики (Policy Decision Point, PDP) и точка применения политик к потокам данных (Policy Enforcement Point, PEP). Атрибуты субъектов, объектов и среды функционирования находятся в хранилище, называемом Policy Information Point (PIP). Точка администрирования политики (Policy Administration Point, PAP) — предоставляет пользовательский интерфейс для создания, управления, тестирования и отладки политик, а так же сохранения этих политик в соответствующем хранилище [3].

Типичный пример работы ABAC предприятия выглядит следующим образом (рис.2):

Пользовательский компьютер направляет запрос к защищенному с помощью определенной политики ресурсу. Далее PEP направляет запрос к точке принятия решения (PDP). Основываясь на данных, полученных в запросе и дополнительных атрибутах субъекта, объекта, действия и среды, PDP принимает решение о предоставлении или отказе

пользователю в доступе. Ответ, также составленный на языке разметки контроля доступа, направляется к PEP, что, в свою очередь, открывает пользователю доступ или отказывает в нем.

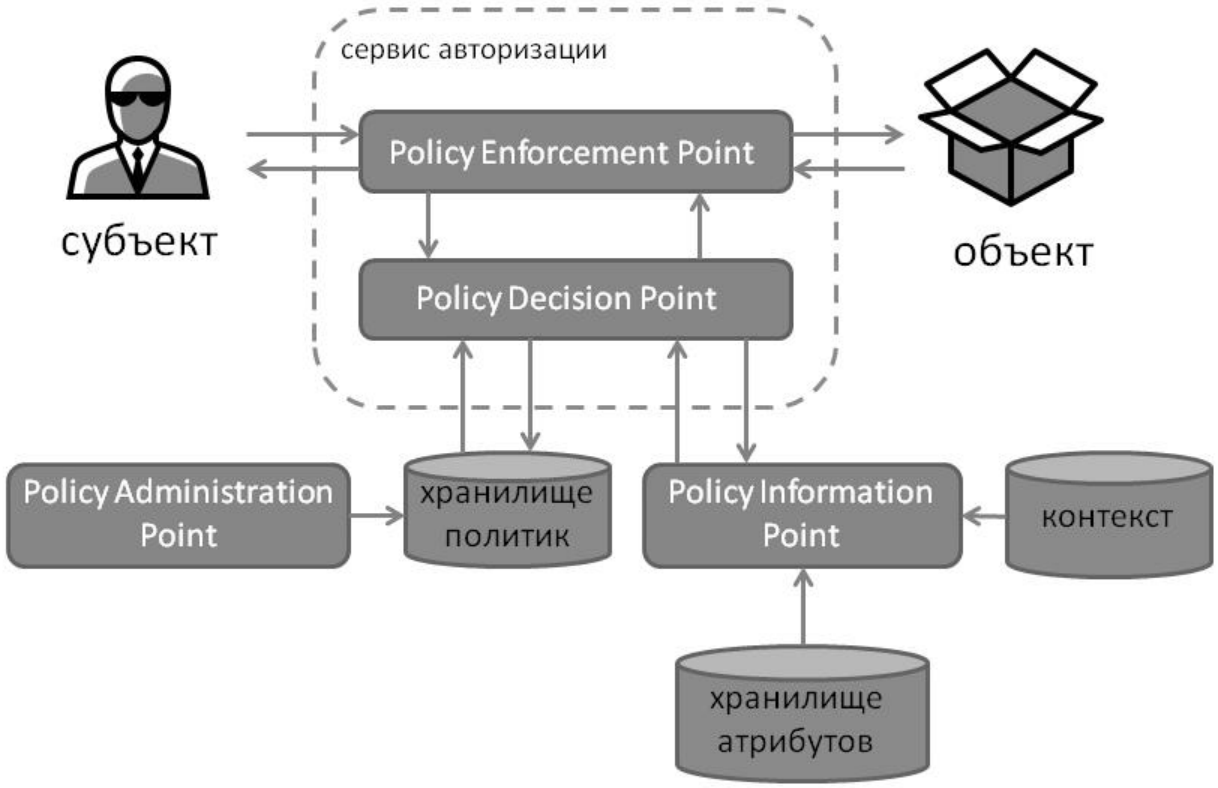

Рис.2. Пример работы ABAC предприятия.

На сегодняшний день для ABAC существует стандарт XACML, который реализует этот механизм. XACML (англ. eXtensible Access Control Markup Language - расширяемый язык разметки контроля доступа) — основанный на языке XML стандарт, разработанный OASIS, определяющий язык описания политик управления доступом, модель и способы их обработки. Этот стандарт описывает необходимые компоненты системы, их назначение, способ их взаимодействия и использования.

Функциональные точки PDP и PEP могут быть централизованы или распределены, могут быть физически и логически отделены друг от друга. Например, предприятие может создать централизованно управляемую службу решений, которая оценивает атрибуты и политики и вычисляет решения, которые затем передаются в PEP. Другой вариант, локальные организации внутри предприятия могут реализовать отдельные PDPs, которые пользуются централизованным хранилищем политик (правил) [3].

Даже в небольшой закрытой системе ABAC опирается на присвоенные субъекту и объекту атрибуты и разработку политики, которая содержит правила доступа. Каждому объекту внутри системы и каждому субъекту, который использует систему, должны быть присвоенные особые атрибуты, которые его характеризуют. Каждый объект в рамках системы должен иметь, по крайней мере, одну политику, которая определяет правила доступа. Такая политика, как правило, происходит от документированных или процедурных правил, описывающих бизнес-процессы и допустимые действия в рамках организации. После того, как атрибуты объекта, атрибуты субъекта и политика установлены, объекты могут быть защищены с помощью ABAC.

Политики, которые могут быть реализованы в модели ABAC, ограничены только возможностями программного языка и богатством доступных атрибутов. Эта гибкость позволяет наибольшей области субъектов получить доступ к наибольшей области объектов

без указания индивидуальных отношений между каждой парой субъект-объект. Так как атрибуты могут отразить надлежащим образом подробную информацию о всех сущностях, *ABAC* обеспечивает большую гибкость в выражении детальной политики и большую гибкость настройки. Соответствующие атрибуты могут охватывать списки контроля доступа (DAC), метки безопасности, разрешения и классификации (MAC) и роли (RBAC). Вдобавок к гибкости, атрибуты и их значения могут быть изменены на протяжении всего жизненного цикла субъектов, объектов и атрибутов.

Принципиально важным преимуществом модели ABAC является тот факт, что субъект доступа совершенно не обязательно должен быть заранее зарегистрирован в системе: необходимым является исключительно наличие у него соответствующих атрибутов [6]. Когда в организации появляются новые субъекты, нет необходимости изменять правила и атрибуты объектов. Пока субъекту назначены атрибуты, необходимые для доступа к требуемым объектам, никаких изменений к существующим правилам или атрибутам объектов не требуется. Это преимущество часто называются «адаптацией к внешним (непредвиденным) пользователям».

Таким образом, эта модель позволяет создавать универсальные политики безопасности, обладая необходимыми возможностями по надежному ограничению несанкционированного доступа к объектам, при этом обеспечивая необходимую доступность информации.

Поддержка организационных решений и разграничение доступа

Современная СППР это сложная и динамичная система, которая учитывает множество факторов, тем больше потребность в гибкости ее подсистем. Дэниэл Повер [2] определят такие основные атрибуты современной СППР: интегрированные системы с комплексной архитектурой; очень большие хранилища данных; множество одновременно работающих пользователей; многократное использование; множество источников данных, включая мультимедиа и он-лайн данные; множество форм доступа и оперирования для пользователей; ориентация на выполнение задач, влияние на идентификацию и принятие решений.

Исследования [11] в среде автоматизированной поддержки организационных решений в современных организациях показали, что особенностями функционирования данной среды являются: динамичность приоритетов и контекстов; распределенность необходимых знаний об объекте управления среди представителей разных бизнес-ролей; включение в число пользователей всех лиц, непосредственно или опосредованно влияющих на качество и эффективность принимаемого решения; необходимость активного использования всех информационных ресурсов организации; максимальное использование контекста; критичность всех этапов процесса принятия решения для его качества; а также необходимость сохранения и распространения знаний, приобретенных в процессе, для последующего семантически актуального доступа всех полученных результатов.

Современные особенности и характеристики СППР ставят задачи защиты конфиденциальности, доступности и целостности данных, комплексного разграничения доступа к данным и динамичного управления доступом.

При создании подсистемы защиты данных и управления доступом в современных СППР поддержки конфиденциальности, простых операций (чтение, запись), одномерных бизнес-правил и распределения всех данных по неизменным уровням безопасности не достаточно. Важно поддерживать целостность и доступность данных, еще важнее обеспечить динамичность и гибкость всех подсистем доступа, возможность динамичной смены полномочий, а так же автоматическое распределение данных по грифам секретности, особенно для систем с централизованным хранилищем, в которых обрабатывается как секретная, так и открытая информация.

Требования к подсистеме управления доступом в современных СППР нельзя выполнить с помощью статичных моделей. Механизм ABAC благодаря своим преимуществам способен реализовать разграничение доступа к разным данным среди разных

участников процесса принятия решения, входящих в процесс на разных этапах с динамичной сменой полномочий. ABAC учитывает контекст, динамичность среды и полностью реализует гибкий, но надёжный контроль доступа.

Заключение

В технологии поддержки организационных решений требуется контекстно-зависимый, гибкий, всеохватывающий, но надёжный контроль доступа, и это те задачи, которые ABAC способен решить. Предлагаемая модель управления доступом объединяет в себе базовые модели, что более важно, она расширяет их с помощью детальных политик авторизации; политики, которые могут быть реализованы в модели ABAC, ограничены только возможностями программного языка и богатством доступных атрибутов.

Большинство работ по моделям атрибутного управления доступом ориентированы на реализацию или оптимизацию подсистемы управления доступом и датированы 2005 – 2014. Так же есть работы по поддержке атрибутивной модели доступа с помощью онтологий. В этой области требуется еще много исследований, так как нет стандартной реализации ABAC. Кроме того исследовательская компания, специализирующаяся на рынках информационных технологий, Gartner прогнозирует [12], что к 2020 году, 70% бизнес-предприятий будут использовать ABAC для авторизации.

В дальнейшем планируется разработка модели управления доступом в СППР на основе атрибутов с учетом таких функциональных особенностей данной среды как динамичность, привязка полномочий к процессу, максимальное использование контекста, необходимость учитывать все факторы влияющие на решение и др. Модель должна решать задачи фильтрации данных, динамической смены полномочий и автоматического распределения поступающих данных.

Литература

1. Голиков С. Е. Выбор модели управления доступом систем автоматизации банковской деятельности / С. Е. Голиков, Н. В. Серова-Нашева // Збірник наукових праць Севастопольського національного університету ядерної енергії та промисловості. - 2013. - № 4. - С.177-185.

2. Power, D. J. What is a modern decision support system? [Електронный ресурс]: article Prof. Daniel J. Power, 27.12.2007. DSSResources.COM // – Режим доступа: http://dssresources.com/ faq/index.php?action =artikel&id=154.

3. Hu Vincent. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. [Електронный ресурс]: National Institute of Standards and Technnology, 2014. NIST Special Publication 800-162 // – Режим доступа: http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

4. Амелин Р.В. Информационная безопасность [Электронный ресурс]: // – Режим доступа: http://nto.immpu.sgu.ru/sites/default/files/3/__77037.pdf

5. The World's Technological Capacity to Store, Communicate, and Compute Information. Martin Hilbert, Priscila Lopez, Science Vol. 332 no. 6025 pp. 60-65 – 2011

6. Марков А.С. Методы оценки несоответствия средств защиты информации / А.С.Марков, В.Л.Цирлов, А.В.Барабанов. - М.: Радио и связь, 2012. 192 с.

7. Ferraiolo D. Role-Based Access Controls / David F. Ferraiolo, D. Richard Kuhn. – National Institute of Standards and Technology, 15th National Computer Security Conference. - 1992. - pp. 554–563.

8. Elliott A. A. Role Explosion: Acknowledging the Problem / A. A. Elliott and G. S. Knight. - Software Engineering Research and Practice, CSREA Press. – 2010. – pp. 349-355.

9. Xin J. Attribute Based Access Control Models (ABAC) and Implementation in Cloud Infrastructure as a Service [Электронный ресурс]: diss. Xin Jin 2014. // [Режим доступа]: http://profsandhu.com/ dissert/ Dissertation_Xin_Jin.pdf

10. Xin J. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. / Xin Jin, Ram Krishnan and Ravi Sandhu. - 26th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSEC). – 2012. – pp. 41-55.

11. Ильина Е.П. Принципы построения интеллектуальной информационной технологии поддержки решений в организации / Ильина Е.П., Синицын И.П., Яблокова Т.Л. // Проблеми програмування. – 2015. - № 2. – С. 63-75.

12. http://www.avatier.com/ [Электронный ресурс]: // [Режим доступа]: http://www.avatier.com/ products/identity-management/resources/gartner-iam-2020-predictions (12.06.2015)

Надійшла 05.06.2015 р. Рецензент: д.т.н., проф. Хорошко В.О.