Математические структуры и моделирование 2018. № 2(46). С. 135–152

УДК 004.056
DOI: 10.25513/2222-8772.2018.2.135-152

АНАЛИЗ ПРОБЛЕМ УПРАВЛЕНИЯ РАЗГРАНИЧЕНИЕМ ДОСТУПА В КРУПНОМАСШТАБНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Н.Ф. Богаченко
к.ф.-м.н., доцент, e-mail: nfbogachenko@mail.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. В статье рассматриваются общие вопросы управления разграничением доступа к ресурсам крупномасштабных информационных систем (КМИС) с позиций формальных математических моделей. Анализируются свойства, присущие КМИС, и требования, предъявляемые к её политике безопасности, реализующей методы и правила разграничения доступа. Ставится задача разработки новых моделей, методов и алгоритмов управления разграничением доступа в КМИС.

Ключевые слова: разграничение доступа, политика безопасности, администрирование, автоматизация.

Введение

В настоящее время информационные системы и информационные технологии являются основой деятельности практически любого предприятия или организации. Согласно [37], информационные технологии — это «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов». Информационная система определяется как «совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств» [37]. Таким образом, термин «информационная система» объединяет информационные ресурсы, программное обеспечение и компьютерное оборудование. В частности, крупные информационные системы, предназначенные для бизнеса, получили название «корпоративные информационные системы».

Принято различать три уровня функционирования объектов информатизации, обслуживаемых информационными системами:

1) микроуровень (учреждение, организация, предприятие);

2) мезоуровень (область, регион, отрасль);

3) макроуровень (государство, межгосударственная структура).

Наиболее востребованными являются информационные системы, обеспечивающие функционирование объектов 2-го и 3-го уровней. Как правило, это

масштабные, распределённые программно-технические комплексы с развитыми коммуникационными связями, обеспечивающие работу связанной группы организаций или предприятий. Такие системы принято называть *крупномасштабными информационными системами* (КМИС)[1].

Цель данной статьи — выявить основные проблемы, возникающие при разграничении доступа к информационным ресурсам КМИС, и определить пути их решения.

1. Крупномасштабные информационные системы и основы защиты информации

Можно выделить несколько причин появления и всё большего распространения КМИС.

1. Потребности бизнеса и государства во взаимодействии, в интеграции разрозненных информационных систем, обслуживающих эти структуры.

2. Потребности в расширении возможностей информационных систем управления ресурсами предприятия (Enterprise Resource Planning Systems, ERP-систем). Технологии развиваются в направлении выделения ядра ERP и создания дополнительных, например облачных, сервисов, специализированных приложений. Всё большее распространение приобретает мультивендорная стратегия, когда в одной информационной системе интегрируется программное обеспечение разных производителей.

3. Развитие концепции цифрового предприятия. Для цифрового предприятия важную роль играют удобные, безопасные, конкурентоспособные электронные ресурсы и информационные сервисы по работе с клиентом.

Использование КМИС позволяет вывести деятельность предприятий и организаций на качественно новый уровень производства и управления. Но в то же время их бизнес-процессы становятся чрезвычайно зависимыми от рисков и последствий сбоев применяемых информационных систем. Современные КМИС содержат тысячи или даже миллионы взаимодействующих компонентов аппаратного и программного обеспечения, в связи с чем возникает множество технических и организационных проблем — некоторые из них существовали ранее и теперь стали критическими, а другие возникли в последнее время в результате увеличения масштаба и степени взаимосвязи информационных подсистем.

Одним из основных источников возникающих проблем является уязвимость КМИС для вредоносных атак, направленных на реализацию угроз информационной безопасности [10]. Пробелы в безопасности КМИС могут приводить не только к нарушению конфиденциальности, потере, изменению или уничтожению информации, но и к сбою системы в целом, крупным финансовым и имиджевым потерям. Этому способствуют *масштабность*, *сложность* и *разнородность* крупномасштабных систем.

[1] В англоязычных источниках имеется аналог этого понятия — Large-Scale Complex IT Systems [57, 70].

1. По определению масштаб является отличительной чертой КМИС. Основные метрики измерения масштаба — это количество компонентов, содержащихся в системе, и количество пользователей, поддерживаемых системой.

2. Компоненты КМИС взаимодействуют и обмениваются информацией множеством способов, с многочисленными циклами обратной связи. Сбои в одной части системы могут непредсказуемым образом сказаться на работе КМИС в целом.

3. КМИС нередко создаются на основе объединения нескольких информационных подсистем. Этот процесс приводит к высокому уровню гетерогенности в системах и повышает потребность в функциональной совместимости между компонентами. При этом применение централизованного способа проектирования «сверху вниз» не всегда возможно. Часто КМИС представляет собой результат восходящей интеграции ряда отдельных подсистем.

Таким образом, дополнительные уязвимости КМИС связаны, в частности, с существенным ростом числа пользователей системы, наличием запутанных, плохо отслеживаемых информационных потоков, с распределённостью системы и необходимостью сопряжения подсистем с различными подходами к обеспечению информационной безопасности.

В свою очередь, одним из основных способов защиты информации является защита от несанкционированного доступа (НСД) [37]. Согласно [11], комплекс программно-технических средств и организационных мер по защите информации от НСД должен включать в себя подсистему управления доступом практически для всех классов информационных систем. При этом реализация дискреционного принципа контроля доступа относит используемые средства вычислительной техники ко 2-й группе защищённости, а реализация ещё и мандатной модели — к более защищённой 3-й группе [12]. В этом же документе поясняется, что «применение <...> средств криптографической защиты информации <...> может быть использовано для повышения гарантий качества защиты» [12]. Таким образом, наиболее распространённым и востребованным методом обеспечения конфиденциальности данных является управление доступом к ресурсам информационной системы. Стандарт ISO/IEC 27001/27002 также предусматривает в качестве основных мер защиты разграничение доступа пользователей к информационным ресурсам [27, 28].

С теоретической точки зрения классические и развивающиеся модели безопасности компьютерных систем строятся, исходя из понятия доступа субъекта к объекту, так как базируются на основной аксиоме компьютерной безопасности: «Все вопросы информационной безопасности в компьютерной системе определяются доступами субъектов к объектам»[2] [14]. Набор правил разграничения доступа в информационной системе, который принято называть *политикой разграничения доступа* (*политикой управления доступом*), определяет основные принципы регулирования использования всех ресурсов системы.

Вышесказанное обосновывает утверждение о том, что задача адекват-

[2]Субъекты — это абстрактное представление активных сущностей системы (процессов, потоков, пользователей). Объекты — пассивные сущности системы (области памяти, файлы и т. д. — любые наборы данных, к которым можно обращаться как к целому).

ного построения политики разграничения доступа является не менее важной, чем, например, стойкость используемых криптографических алгоритмов. Программно-технические средства, реализующие политику разграничения доступа КМИС, составляют *подсистему разграничения доступа* (*подсистему управления доступом*). Использование формальных моделей разграничения доступа на всех этапах жизненного цикла этой подсистемы обеспечивает успешное решение задачи выбора и обоснования механизмов реализации средств и методов защиты информационных ресурсов КМИС от несанкционированного доступа (см. рис. 1).

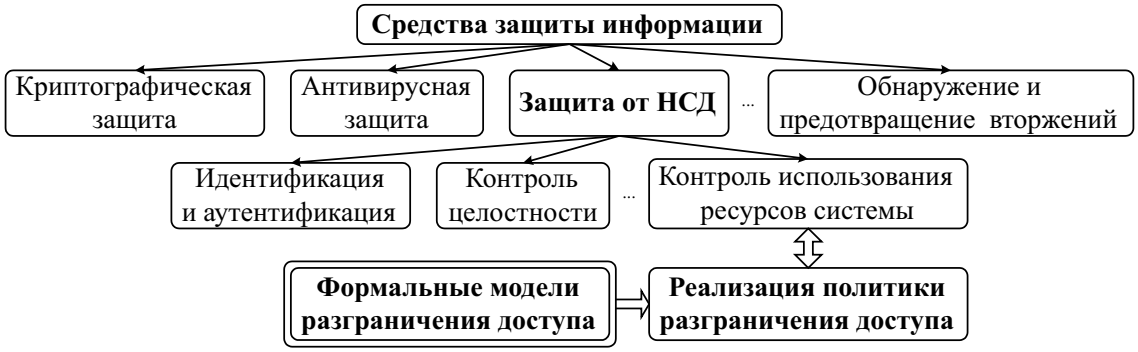

Рис. 1. Место формальных моделей разграничения доступа в системе комплексной защиты информации

2. Теоретические и практические подходы к разграничению доступа

Основы моделирования безопасного управления доступом и информационными потоками заложены в дискреционном (Discretionary Access Control, DAC) [47,51,52,60], мандатном (Mandatory Access Control, MAC) [46,62] и ролевом (Role-Based Access Control, RBAC) [49,50,67,68] принципах разграничения доступа. Классические формальные модели разграничения доступа получили широкое развитие и в работах российских исследователей [8,14,18,21,31,39] и др.

Вместе с тем практическая реализация классических моделей разграничения доступа в современных КМИС сталкивается с существенными трудностями [20]. Появляются, исследуются и находят практическое применение развивающиеся модели разграничения доступа. Развитие дискреционной модели связано с расширением понятия матрицы доступов: от типизированной (Typed Access Matrix, TAM) [66] через динамическую типизированную (Dynamic-Typed Access Matrix, DTAM) [71] до атрибутной (Attribute-Based Access Matrix, ABAM) [76]. В работах [15–17, 19, 23] предлагается ДП-расширение дискреционной, мандатной и ролевой моделей. ДП-модели основаны на иерархии сущностей компьютерной системы. Данный подход позволяет проводить формальный анализ безопасности информационных систем с учётом инфор-

мационных потоков по памяти или по времени, динамических ограничений и возможности кооперации субъектов. Ролевой принцип управления доступом получил развитие в виде моделей логического разграничения доступа. В работе [26] приводятся результаты сравнительного анализа трёх современных моделей логического разграничения доступа: атрибутной модели (Attribute-Based Access Control, ABAC) [38, 41, 53], сущностной модели (Entity-Based Access Control, EBAC) [1, 48] и реляционной модели на основе цепочек отношений, предложенной авторами для многопользовательских информационно-аналитических систем [6]. Управление доступом на основе задач (Task-Based Access Control, TBAC) — ещё одно направление развития ролевого подхода [26, 73]. Ряд работ посвящён оптимизации иерархических структур ролевой модели [5, 44, 55, 56, 58, 72, 74, 77]. Развитие получила так называемая проблема разработки ролей (Role Mining Problem, RMP), относящаяся к задачам интеллектуального анализа данных и использующая восходящий принцип проектирования политики ролевого разграничения доступа [2, 59, 61, 63, 69, 75]. Ведутся исследования по совмещению нескольких классических подходов в одной политике разграничения доступа [3, 4, 22, 24, 29, 45, 54, 64]. Наблюдается повышенный интерес к формальным моделям и методам разграничения доступа к информационным ресурсам в распределённых системах и облачных сервисах [13, 40, 42, 43, 65, 78].

Вместе с тем анализ современных работ, касающихся вопросов разграничения доступа, свидетельствует, что наряду с имеющимися существенными достижениями в области построения формальных моделей, методов и алгоритмов управления доступом к информационным ресурсам, методологические подходы к обеспечению безопасного управления доступом к объектам КМИС требуют дополнительных теоретических исследований с позиций масштабности, сложности и разнородности информационных систем.

В области реализации политик разграничения доступа активно ведутся программно-технические разработки. Системы управления доступом (СУД)[3] представляют собой современные программно-технические комплексы, позволяющие решать ряд проблем, связанных с управлением доступом к информационным ресурсам КМИС. В качестве примеров таких систем можно указать следующие автоматизированные решения: СУД компании «Энкор» [32]; программное обеспечение по управлению доступом на основе криптографических алгоритмов компании «АВТОР» [34]; СУД компании «Куб», использующая специализированный документооборот заявок [33]; система управления идентификационными данными и доступом компании «Индид»; IBM Tivoli Identity Manager; Oracle Identity Management [35] и др.

Основная задача этих систем — автоматизация процессов управления пользователями, ролями, идентификационными данными, правами доступа. Преимущество автоматизированных решений заключается, в частности, в следующем:

[3]Более общие программные решения носят название «системы управления идентификационными данными и доступом пользователей» (Identity and Access Management System, IAMS) [36].

1) снижение вероятности ошибок при администрировании и, как следствие, снижение рисков информационной безопасности;

2) увеличение быстродействия за счёт сокращения времени предоставления доступа;

3) повышение производительности;

4) снижение накладных расходов.

Вместе с тем современные СУД обладают рядом недостатков. Во-первых, новые доступы регламентируются на основе предварительно настроенных политик и шаблонов. При появлении в системе нового пользователя к нему применяется один из заготовленных шаблонов пользовательских разрешений. Для КМИС доля шаблонов, задаваемых администратором безопасности «в ручном» режиме, будет существенной и потребует больших временных затрат. Объясняется это тем, что чем масштабнее объект, обслуживаемый информационной системой, те более специфичны его бизнес-процессы, следовательно, более индивидуальна система разграничения доступа. Здесь возникает и вторая проблема — разрастание базы данных шаблонов, что требует дополнительных ресурсов.

Во-вторых, шаблоны создаются и корректируются, исходя из анализа бизнес-процессов. Тем самыми используется нисходящая технология проектирования, что для крупномасштабных систем не всегда эффективно. При изменении бизнес-процессов, что неизбежно для КМИС с достаточно продолжительным жизненным циклом, отсутствие необходимых шаблонных разрешений может привести к утрате конфиденциальности или доступности информации. Одним из способов решения указанных проблем является построение адаптивной системы управления разграничением доступа [7], которая сможет автоматически подстраиваться под изменяющиеся параметры системы.

В-третьих, такое преимущество СУД, как интеграция с кадровыми сервисами компании, применительно к КМИС не всегда даёт положительный результат. По сути происходит отождествление управленческой иерархии компании с иерархией ролей политики разграничения доступа, которую предлагает СУД. Данный подход эффективен в ситуации, когда все подразделения в компании разные. Если же в иерархии имеются схожие подструктуры, то может происходить дублирование ролей или порождение ролей с «близкими» наборами полномочий. Это в свою очередь приводит к необходимости пополнения функционала СУД механизмами оптимизации иерархической структуры доступа.

Наконец, следует отметить, что основным подходом к разграничению доступа в СУД является ролевая модель. Вместе с тем на практике при построении подсистемы разграничения доступа КМИС нередки ситуации, требующие совместной реализации нескольких принципов разграничения доступа. К сожалению, вопросы автоматизации процессов управления доступом на основе мандатных и дискреционных подходов не получили должного развития в современных СУД.

Вышесказанное позволяет сделать вывод о том, что на сегодняшний день отсутствует единый подход к решению проблем, возникающих в процессе эксплуатации СУД. Очевидно, что современные технологии разграничения доступа к информационным ресурсам должны развиваться с учётом особенностей КМИС.

При этом разработка и реализация программно-технических решений, повышающих уровень безопасности и надёжности КМИС, должна быть поддержана дополнительными исследованиями фундаментальных вопросов информационной безопасности крупномасштабных систем, включающих в себя разработку новых моделей, методов и алгоритмов *автоматизации* процессов *управления разграничением доступа* к информации, то есть процессов построения и сопровождения (администрирования) политики разграничения доступа.

Для постановки основных задач, возникающих в процессе управления разграничением доступа в КМИС, необходимо:

1) выделить основные свойства (признаки) КМИС;

2) определить особенности разграничения доступа к информации в КМИС;

3) выявить существующие алгоритмические проблемы разработки политики разграничения доступа КМИС.

3. Особенности разграничения доступа к информации в крупномасштабных информационных системах

Растущее число проблем, возникающих при работе подсистемы разграничения доступа КМИС, объясняется от части тем, что вопросы управления доступом пользователей к информационным ресурсам находятся на стыке двух процессов: обеспечение безопасности и автоматизация [30]. При этом темпы разработки и внедрения КМИС настолько высоки, что детальной проработке функционала подсистемы, реализующей политику разграничения доступа, часто не уделяется должного внимания. Нередко обеспечение бизнес-процесса (то есть возможности получения доступа пользователя к приложению) получает больший приоритет, чем выполнение правил политики безопасности.

Вместе с тем существует ряд проблем, которые следуют из особенностей самих КМИС. Построение эффективной подсистемы разграничения доступа к информационным ресурсам КМИС требует особых подходов. Традиционные методики, методы и алгоритмы решения поставленной задачи ориентированы главным образом на обеспечение информационной безопасности объектов информатизации 1-го уровня. Чтобы определить специфику, присущую КМИС, требуется выделить и проанализировать основные свойства больших систем вообще, и КМИС в частности.

Общепринято считать, что определяющими свойствами большой системы (не обязательно информационной) являются масштабность, сложность и разнородность. Этот набор признаков следует детализировать. Согласно [9, 25], большие системы обладают следующими характерными свойствами:

1) наличие в системе подсистем, каждую из которых можно рассматривать как отдельную систему;

2) определение для каждой подсистемы иерархии целей и выполняемых функций;

3) выделение и декомпозиция процессов, связывающих подсистемы в единую структуру;

4) гетерогенность системы: мультизадачность элементов, различная природа внешних воздействий и выходных данных, многообразие ресурсов и информационных потоков;

5) системный подход к проектированию — необходима целостная концепция функционирования и развития предметной области, для которой создаётся система;

6) индивидуальность — большая система разрабатывается для вполне определённого объекта мезо- или макроуровня и содержит массу специфических черт;

7) продолжительность разработки и внедрения, как следствие — потребность в сопровождении.

Вышеперечисленные свойства необходимо конкретизировать применительно к КМИС. В работе [7] на примере государственных информационных систем приведено обоснование принадлежности КМИС к сложным адаптивным системам и выделены основные признаки КМИС.

1. Большой территориальный размах.

2. Сложное динамическое поведение.

3. Наличие разнородных, сложно взаимодействующих информационных элементов (узлов).

4. Многоуровневая иерархическая структура.

5. Многоцелевой характер управления и функционирования.

6. Наличие коллектива людей, осуществляющего управление.

7. Вероятностное внешнее воздействие.

8. Продолжительный жизненный цикл (время создания, период функционирования и эволюции).

Наиболее значимыми с точки зрения влияния на подсистему безопасности КМИС являются первые 4 свойства.

Указанные признаки обусловливают особенности в управлении доступом к информационным ресурсам КМИС. В [36] приведён перечень основных характеристик подсистемы безопасности КМИС: «Большое количество пользователей; разнообразие прикладных программ; разрозненные механизмы и политики доступа для различных ресурсов; большой объём обрабатываемой информации; отсутствие механизмов централизованного управления учётными записями; неконтролируемая деятельность привилегированных пользователей; необходимость соблюдения нормативных требований и обеспечения аудита». Для подсистемы разграничения доступа КМИС определяющими будут являться следующие особенности.

1. Существенное увеличение числа пользователей и объектов.

Информационные системы подразделяются на классы в зависимости от сложности решаемых ими задач и от числа поддерживаемых ими пользователей. Именно число пользователей, для которых данная система доступна, определяет её масштаб. Число пользователей и ресурсов КМИС в несколько раз превосходит эти показатели для информационных систем микроуровня. При построении подсистемы разграничения доступа необходимо учесть максимальное количество вариантов доступа. Следовательно, в КМИС число ос-

новных элементов подсистемы разграничения доступа таких, как роли, метки безопасности и т. д., также существенно возрастает.

2. Изменяемость политики разграничения доступа.

В силу сложного динамического поведения КМИС её подсистема разграничения доступа также должна приспосабливаться к изменяемым параметрам объектов и внешней среды.

3. Необходимость совмещения политик разграничения доступа.

Нередко КМИС разрабатывается не «с нуля», а строится из уже существующих отдельных компонент, часто разных производителей с разным подходом к разграничению доступа. Ситуация осложняется тем, что многие производственные процессы являются непрерывными, их нельзя приостановить для существенной модернизации или замены используемого программного обеспечения. Таким образом, подсистема разграничения доступа КМИС должна унаследовать принципы и методы разграничения доступа отдельных компонент, включённых в единую информационную систему.

4. Распределённость и иерархичность объектов доступа.

Большинство КМИС распределены в пространстве. При этом элементы (узлы) КМИС могут объединяться в сложную многоуровневую иерархическую структуру.

Перечисленные характеристики подсистемы разграничения доступа КМИС позволяют выделить и формализовать основные проблемы, возникающие в процессе управления разграничением доступа.

4. Проблемы управления разграничением доступа в крупномасштабных информационных системах

Большое число пользователей и ресурсов, изменяемость состава пользователей КМИС, территориальная распределённость приводят к возникновению множества подзадач администрирования, а, значит, повышается риск возникновения ошибок. Примерами могут являться неверное или несвоевременное назначение / лишение прав доступа, неправомерное использование идентификационных данных, нарушение правил политики безопасности и т. д. При этом автоматизация процессов распределения прав и полномочий пользователей чаще всего ограничивается установками «по умолчанию». Дальнейшее управление разграничением доступа проводится администратором безопасности «в ручном» режиме. Такой подход имеет ряд недостатков. В частности, злоумышленник может знать схему «по умолчанию», а сама схема требует большого объёма доопределений и индивидуальных настроек. Это приводит к востребованности алгоритмов, позволяющих частично или полностью автоматизировать процессы установки и администрирования прав доступа.

В связи с существенным увеличением числа пользователей и объектов КМИС и изменяемостью её политики разграничения доступа традиционный нисходящий подход к проектированию политики разграничения доступа сталкивается с трудностями на этапе реализации. Получает распространение восходящий принцип построения политики. В силу большого объёма информации,

необходимой для анализа КМИС, этот подход не может быть реализован в ручном режиме. Поэтому актуальной является задача разработки алгоритмов автоматизации процессов формирования политики разграничения доступа на основе подхода «снизу вверх».

Основная проблема, обусловленная изменяемостью политики разграничения доступа КМИС, — достаточно спонтанная эволюция политики, которая приводит к запутыванию существующих информационных потоков между сущностями системы, появлению дублирующих сущностей и т. п. Следствием этого является рост рисков утечки прав доступа. Подобные проблемы могут решаться за счёт оптимизации основных структур политики разграничения доступа в соответствии с новыми требованиями. При этом оптимальность должна пониматься в широком смысле как характеристика наиболее эффективной работы системы. Очевидно, что задача такой оптимизации многокритериальна, часть критериев могут противоречить друг другу. К сожалению, в большинстве современных информационных систем при реализации той или иной модели разграничения доступа вопросам оптимальности уделяется внимание лишь на этапе проектирования. Тогда как перестройка (оптимизация) политики разграничения доступа должна представлять собой итеративный процесс, основывающийся на непрерывном формировании новых и уточнении существующих требований предметной области.

В ситуации, когда КМИС создаётся на основе объединения нескольких информационных систем, каждая — со своей политикой разграничения доступа, — ставится задача совмещения действующих политик при условии безостановочного режима работы всех подсистем. В этом случае остро стоит вопрос эффективности процесса совмещения как с точки зрения информационной безопасности, так и с позиции затрат времени и человеческих ресурсов. Традиционный подход основан на поиске идеального решения, удовлетворяющего требованиям всех совмещаемых политик разграничения доступа. Но для крупномасштабных систем такое идеальное решение чаще всего не существует. Актуальным представляется использование алгоритмов поддержки принятия решений, позволяющих учесть ограничения совмещаемых политик разграничения доступа.

Кроме того, совмещение подходов к разграничению доступа приводит к ряду проблем, связанных с неоптимальностью результирующей модели разграничения доступа: увеличение времени на принятие решения о предоставлении или запрете доступа, появление противоречивых правил разграничения доступа. Последнее может приводить к отклонениям от политики разграничения доступа и, как следствие, к повышению рисков утечки прав и полномочий. В связи с этим по-прежнему актуальной остаётся указанная ранее задача разработки алгоритмов оптимизации информационных структур и правил разграничения доступа в подсистеме безопасности КМИС.

Иерархичность и распределённость объектов доступа КМИС ведёт к востребованности эффективных алгоритмов разграничения доступа к информационным ресурсам в распределённых системах и системах с многоуровневой иерархической структурой. При этом необходимо учитывать, что в распределённой

системе (облаке), как правило, отсутствует единая подсистема безопасности, и разделение доступа достигается с помощью средств шифрования и технологий распределения ключей доступа.

Приведённый перечень актуальных проблем, возникающих при построении и сопровождении политики разграничения доступа КМИС, определяет необходимость разработки новых научно-обоснованных моделей, методов и алгоритмов управления разграничением доступа в условиях обработки больших массивов данных о пользователях и информационных ресурсах. Для достижения поставленной цели требуется решение следующих основных задач (см. рис. 2).

1. Анализ и формализация классических моделей разграничения доступа с учётом особенностей КМИС.

2. Разработка методов и средств автоматизации процессов построения ролевого, мандатного и дискреционного разграничения доступа к объектам КМИС.

3. Разработка методов и средств оптимизации политики разграничения доступа КМИС на основе различных критериев.

4. Разработка методов и средств автоматизации процессов совмещения различных политик разграничения доступа КМИС.

5. Разработка методов и средств построения распределённой политики разграничения доступа КМИС.

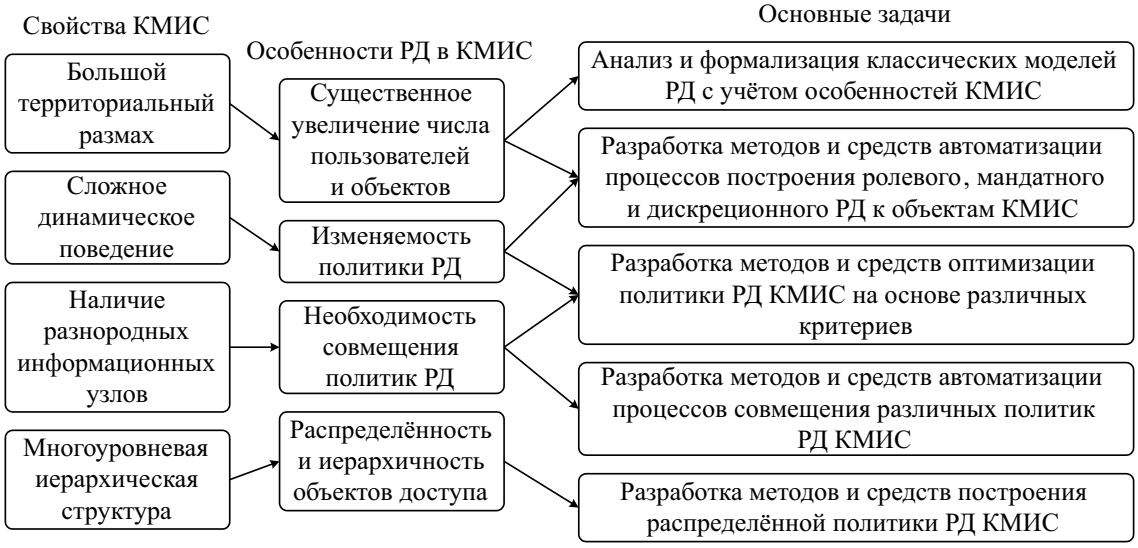

Рис. 2. Связь основных задач с характерными особенностями разграничения доступа (РД) в КМИС

Основное требование к разрабатываемым подходам, моделям, методам, алгоритмам — автоматизация соответствующих процессов построения и сопровождения политики разграничения доступа. Так как полная автоматизация указанных процессов невозможна, в силу рассмотренных ранее свойств крупномасштабных систем, для решения поставленных задач целесообразно использовать подходы, основанные на процессах поддержки принятия решений. В частности, могут быть задействованы метод анализа иерархий и технологии интеллекту-

ального анализа данных (Data Mining). Новые подходы к управлению разграничением доступа должны приводить к построению масштабируемых алгоритмов, способных поддерживать работоспособность по мере увеличения числа пользователей.

Формализация процесса создания любой сложной системы представляет собой циклический (итерационный) процесс. Каждая итерация этого процесса состоит из следующих основных элементов: системный анализ, проектирование, реализация, сопровождение. Именно на этапе сопровождения могут быть сформулированы дополнительные требования к системе, направленные на её оптимизацию, получение нового или добавочного качества, повышение гибкости и способности к адаптации. Жизненный цикл политики разграничения доступа КМИС также должен включать в себя как стадию разработки (engineering) — постановка задачи, системный анализ, проектирование и реализация, так и стадию реконструкции (re-engineering) — администрирование, анализ и оптимизация. Следует отметить, что сформулированные задачи исследований в области управления разграничением доступа к ресурсам КМИС охватывают все этапы жизненного цикла политики разграничения доступа.

Заключение

Технологии управления доступом к информационным ресурсам должны основываться на формальных моделях и методах разграничения доступа, учитывающих масштабность, сложность и разнородность современных информационных систем.

На современном уровне развития СУД администрирование политики разграничения доступа характеризуется тем, что большинство операций по управлению разграничением доступа осуществляется администратором безопасности «в ручном режиме» или задаётся «по умолчанию» и через шаблонные решения. Это приводит к появлению ряда проблем при работе с КМИС.

Выявленные проблемы в построении и сопровождении политики разграничения доступа КМИС актуализируют разработку новых моделей, методов и алгоритмов, позволяющих частично или полностью автоматизировать процессы управления разграничением доступа в КМИС на всех этапах жизненного цикла политики разграничения доступа.

Автоматизация процессов управления разграничением доступа пользователей к ресурсам позволит повысить быстродействие и производительность СУД и снизить риски информационной безопасности за счёт снижения вероятности ошибок администрирования. При этом возможность автоматизации будет заложена в сами подходы к построению политики разграничения доступа, что позволит разрабатывать более надёжные и прогнозируемые СУД.

Литература

1. Афонин С.А. Система логического разграничения доступа для облачных информационных систем // Научный сервис в сети Интернет: труды XVIII Всероссий-

ской научной конференции (19-24 сентября 2016 г., Новороссийск). М. : ИПМ им. М.В. Келдыша, 2016. С. 51–57. URL: http://keldysh.ru/abrau/2016/17.pdf (дата обращения: 23.05.2018).

2. Белим С.В., Богаченко Н.Ф. Использование решётки формальных понятий для построения ролевой политики разграничения доступа // Информатика и системы управления. 2018. № 1(55). С. 16–28.
3. Белим С.В., Богаченко Н.Ф., Ракицкий Ю.С. Совмещение политик безопасности, основанное на алгоритмах поддержки принятия решений // Информационно-управляющие системы. 2016. № 5. С. 66–72.
4. Белим С.В., Богаченко Н.Ф., Ракицкий Ю.С. Теоретико-графовый подход к проблеме совмещения ролевой и мандатной политик безопасности // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 9–17.
5. Богаченко Н.Ф. Локальная оптимизация политики ролевого разграничения доступа (Local Optimization of the Role-Based Access Control Policy) // CEUR Workshop Proceedings. 2017. V. 1965. URL: http://ceur-ws.org/Vol-1965/paper14.pdf (дата обращения: 23.05.2018).
6. Васенин В.А., Иткес А.А., Шапченко К.А., Бухонов В.Ю. Реляционная модель логического разграничения доступа на основе цепочек отношений // Программная инженерия. 2015. № 9. С. 11–19.
7. Володина А.А., Лёвкин И.М. Адаптивный подход к защите информации в больших информационных системах // Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур : Межвузовский сборник трудов VI Всероссийской научно-технической конференции КОНФИБ'15. СПб. : Университет ИТМО, 2016. С. 65–73.
8. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. Екатеринбург : Изд-во Урал. ун-та, 2003. 328 с.
9. Горбачев В.Г. Некоторые проблемы создания больших информационных систем в учреждении // Центр системных исследований. Методология. 2009. URL: http://www.inmeta.ru/metod/big_syst.htm (дата обращения: 23.05.2018).
10. Горбачевская Е.Н. Исследование механизмов защиты данных в корпоративных информационных системах // Вестник Волжского университета им. В.Н. Татищева. 2012. № 4(20). С. 18–23.
11. Гостехкомиссия России. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации». Москва, 1992. 29 с.
12. Гостехкомиссия России. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации». Москва, 1992. 21 с.
13. Грушо А.А., Грушо Н.А., Тимонина Е.Е., Шоргин С.Я. Безопасные архитектуры распределённых систем // Системы и средства информатики. 2014. Т. 24, № 3. С. 18–31.
14. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. 2-е изд., испр. и доп. М. : Научно-техническое издательство «Горячая линия — Телеком», 2013. 338 с.
15. Девянин П.Н. О проблеме представления формальной модели политики безопасности операционных систем // Труды ИСП РАН. 2017. Том 29, Вып. 3. С. 7–16.

16. Девянин П.Н. О результатах формирования иерархического представления МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. 2016. № 9. С. 83–87.
17. Девянин П.Н. Обзор семейства ДП-моделей безопасности логического управления доступом и информационными потоками в компьютерных системах // Информационные технологии. 2010. № 5. С. 20–25.
18. Девянин П.Н. Обзорные лекции по моделям безопасности компьютерных систем // Прикладная дискретная математика. 2009. Приложение № 2. С. 151–190.
19. Девянин П.Н. Ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux // Прикладная дискретная математика. 2012. № 1. С. 69–90.
20. Жуковский О.И., Гриценко Ю.Б. Особенности создания системы информационной безопасности веб-ГИС ведения электронного генерального плана инженерной инфраструктуры // Доклады ТУСУР. 2013. № 2(28). С. 101–106.
21. Зегжда Д.П. Общая схема мандатных моделей безопасности и её применение для доказательства безопасности систем обработки информации // Проблемы информационной безопасности. Компьютерные системы. 2000. № 2. С. 28–32.
22. Иткес А.А. Объединение моделей логического разграничения доступа для сложноорганизованных распределённых информационных систем // Проблемы информатики. 2010. № 1, С. 85–94.
23. Колегов Д.Н. Применение ДП-моделей для анализа защищённости сетей // Прикладная дискретная математика. 2008. № 1(1). С. 71–87.
24. Королев И.Д., Поддубный М.И., Носенко С.В. Применение сегмента матрицы доступов ХРУ в анализе информационной безопасности систем, реализующих мандатное разграничение доступа // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2014. № 101. С. 1811–1823.
25. Кротов А.А., Лупян Е.А. Обзор методов реструктуризации и интеграции информационных систем. М. : ИКИ РАН, 2000. URL: `http://smis.iki.rssi.ru/students/alekro/Dissertation/Papers/Reengineering/my_review.html` (дата обращения: 23.05.2018).
26. Лапин С.А. Модель разграничения доступа для систем, содержащих равнозначные объекты // Безопасность информационных технологий. 2016. № 2. С. 49–54.
27. Международный стандарт ISO/IEC 27001. URL: `http://www.pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf` (дата обращения: 23.05.2018).
28. Международный стандарт ISO/IEC 27002. URL: `http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27002-2013.pdf` (дата обращения: 23.05.2018).
29. Оленников А.А., Оленников Е.А., Захаров А.А., Широких А.В., Варнавский В.В. Разработка модели управления доступом для типовой медицинской информационной системы // Программные продукты и системы. 2016. № 1. С. 166–169.
30. Савельев М. Разграничение доступа – долой маски! // Информационная безопасность. 2007. № 4. С. 64–65.
31. Сизоненко А.Б. Арифметико-логическое представление матрицы доступа в дискреционной модели разграничения доступа // Вестник Воронежского института МВД

России. 2012. № 3. С. 201–206.

32. Система управления доступом. URL: https://n-core.ru/projects/solutions/acs.html (дата обращения: 23.05.2018).
33. Система управления доступом. URL: https://www.cube-system.ru/products/sistema-upravleniya-dostupom-rasshiryaet-vozmozhnosti-produkta-kub (дата обращения: 23.05.2018).
34. Системы управления доступом к информационным ресурсам. URL: http://avtor.ua/resheniya/sistemy-upravleniya-dostupom.html (дата обращения: 23.05.2018).
35. Системы управления идентификационными данными и доступом. URL: http://altirix.ru/index.php/products/sistemy-upravleniya-identifikatsionnymi-dannymi-i-dostupom (дата обращения: 23.05.2018).
36. Сова А. Управление идентификационными данными и доступом – основа системы информационной безопасности КИС // Информационная безопасность. 2009. № 3. С. 34–35.
37. Федеральный закон Российской Федерации от 27.07.2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации». URL: http://base.garant.ru/12148555/#friends (дата обращения: 23.05.2018).
38. Чернов Д.В. О моделях логического управления доступом на основе атрибутов // Прикладная дискретная математика. Приложение. 2012. № 5. С. 79–82.
39. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб. : Наука и техника, 2004. 384 с.
40. Ястребов И.С. Управление доступом в распределённых системах // Автоматизация процессов управления. 2010. № 2. С. 48–53.
41. Al-Kahtani M.A., Sandhu R. A Model for Attribute-Based User-Role Assignment // Proceedings of the Computer Security Applications Conference. 2002. P. 353–362.
42. Anitha R., Mukherjee S. Metadata Driven Efficient CRE based Cipher Key Generation and Distribution in Cloud Security // International Journal of Security and Its Applications. 2014. V. 8, No. 3. P. 377–392.
43. Belim S.V., Bogachenko N.F. Distribution of Cryptographic Keys in Systems with a Hierarchy of Objects // Automatic Control and Computer Sciences. 2016. V. 50, No. 8. P. 777–786. URL: urlhttp://link.springer.com/article/10.3103/S0146411616080071 (дата обращения: 23.05.2018).
44. Belim S., Bogachenko N., Ilushechkin E. An analysis of graphs that represent a role-based security policy hierarchy // Journal of Computer Security. 2015. V. 23, No. 5. P. 641–657. URL: http://content.iospress.com/articles/journal-of-computer-security/jcs532 (дата обращения: 23.05.2018).
45. Belim S.V., Bogachenko N.F., Kabanov A.N., Rakitskiy Yu.S. Using the Decision Support Algorithms Combining Different Security Policies // IEEE Dynamics of Systems, Mechanisms and Machines (Dynamics). 15–17 Nov. 2016. URL: http://ieeexplore.ieee.org/document/7818976/ (дата обращения: 23.05.2018).
46. Bell D.E., LaPadula L.J. Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976. MTR–2997 Rev. 1.
47. Bishop M. Applying the Take-Grant Protection Model. Technical Report. Dartmouth College Hanover, NH, USA, 1990. 26 p.

48. Bogaerts J., Decat M., Lagaisse B., Joosen W. Entity-based access control: supporting more expressive access control policies // Proceedings of the 31st Annual Computer Security Applications Conference. ACM, 2015. P. 291–300.
49. Ferraiolo D., Cugini J., Kuhn R. Role-based access control: Features and motivations // Proceedings of Annual Computer Security Applications Conference. IEEE Computer Society Press. 1995. P. 249–255.
50. Ferraiolo D.F., Kuhn D.R. Role-Based Access Controls // Proceedings of 15th National Computer Security Conference. Baltimore MD, 1992. P. 554–563.
51. Harrison M.A., Ruzzo W.L., Ullman J.D. On Protection in Operating Systems // Communications of the ACM. 1975. P. 14–25.
52. Harrison M.A., Ruzzo W.L., Ullman J.D. Protection in Operating Systems // Communications of the ACM. 1976. V. 19, No. 8. P. 461–471.
53. Hu V.C., Ferraiolo D., Kuhn R., Schnitzer A., Sandlin K., Miller R., Scarfone K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations // NIST Special Publication 800-162, January 2014.
54. Kocatürk M.M., Gündema T.I. Fine-Grained Access Control System Combining MAC and RBAC Models for XML // Informatica. 2008. V. 19, Issue 4. P. 517–534.
55. Koch M., Mancini L.V., Parisi-Presicce F. A Graph-Based Formalism for RBAC // ACM Transactions on Information and System Security. 2002. No. 5(3). P. 332–365.
56. Koch M., Mancini L.V., Parisi-Presicce F. Graph-based specification of access control policies // Journal of Computer and System Sciences. 2005. No. 71(1). P. 1–33.
57. Large-Scale Complex IT Systems. Development, Operation and Management / Editors: R. Calinescu, D. Garlan (Eds.). 17th Monterey Workshop 2012. Oxford, UK, March 19–21, 2012.
58. Leitner M. Delta Analysis of Role-Based Access Control Models // Lecture Notes in Computer Science. 2013. V. 8111. P. 507–514.
59. Li N., Li T., Molloy I., Wang Q., Bertino E., Calo S., Lobo J. Role Mining for Engineering and Optimizing Role Based Access Control Systems. Purdue University, IBM T.J. Watson Research Center, 2007.
60. Lipton R.J., Snayder L. A linear time algorithm for deciding subject security // Journal of ACM (Addison-Wesley). 1977. No. 3. P. 455–464.
61. Lu H., Vaidya J., Atluri V. Optimal boolean matrix decomposition: Application to role engineering // Proceedings of International Conference on Data Engineering (ICDE). 2008. P. 297–306.
62. McLean J. The specification and modeling of computer security // Computer. 1990. V. 23, Issue 1. P. 9–16.
63. Molloy I., Li N., Li T., Mao Z., Wang Q., Lobo J. Evaluating Role Mining Algorithms // Proceedings of ACM Symposium on Access Control Models and Technologies (SACMAT). 2009.
64. Ribeiro C., Zuquete A., Ferreira P., Guedes P. SPL: An Access Control Language for Security Policies with Complex Constraints // Proceedings of the Network and Distributed System Security Symposium. Sun Diego, CA. 2001. URL: `https://scholar.google.co.uk/citations?view_op=view_citation&hl=ru&user=3PHaUacAAAAJ&citation_for_view=3PHaUacAAAAJ:LPZeul_q3PIC` (дата обращения: 23.05.2018).
65. Ruj S., Nayak A., Stojmenovic I. DACC: Distributed Access Control in Clouds // Proc.

of IEEE 10th International Conference "Trust, Security and Privacy in Computing and Communications (TrustCom)". 2011. P. 91–98.

66. Sandhu R.S. The Typed Access Matrix Model // Proceedings of IEEE Symposium on Security and Privacy. Oakland, California, 1992. P. 122–136.
67. Sandhu R., Coyne E., Feinstein H., Youman C. Role Based Access Control: A multidimensional view // Proceedings of 10th Annual Computer Security Applications Conference. Orlando, 1994. P. 54–62.
68. Sandhu R.S., Coyne E.J., Feinstein H.L., Youman C.E. Role-Based Access Control Models // IEEE Computer, 1996. No. 29(2). P. 38–47.
69. Schlegelmilch J., Steffens U. Role mining with ORCA // Symposium on Access Control Models and Technologies (SACMAT). 2005.
70. Sommerville I., Cliff D., Calinescu R., Keen J., Kelly T., Kwiatkowska M., McDermid J., Paige R. Large-scale Complex IT Systems // Communications of the ACM. 2011. V. 55(7).
71. Soshi M. Safety Analysis of the Dynamic-Typed Access Matrix Model // Proceedings of the 6th European Symposium on Research in Computer Security. 2000. V. 1895. P. 106–121.
72. Tahir M.N. Hierarchies in Contextual Role-Based Access Control Model (C-RBAC) // International Journal of Computer Science and Security (IJCSS). 2008. No. 2(4). P. 28–42.
73. Thomas R.K., Sandhu R.S. Task-based authorization controls (TBAC: a family of models for active and enterprise-oriented authorization management // Proceedings of the IFIP TC11 WG11.3 Eleventh International Conference on Database Securty XI: Status and Prospects. 1997.
74. Toahchoodee M., Ray I., McConnell R.M. Using Graph Theory to Represent a Spatio-Temporal Role-Based Access Control Model // International Jornal of Next-Generation Computing. 2010. No. 1(2). P. 231–250.
75. Vaidya J., Atluri V., Guo Q. The role mining problem: Finding a minimal descriptive set of roles // Proceedings of Symposium on Access Control Models and Technologies (SACMAT). 2007. P. 175–184.
76. Zhang X., Li Y., Nalla D. ABAM: An Attribute-Based Access Matrix Model // Proceedings of the ACM Symposium on Applied Computing (SAC 2005). Sante Fe, New Mexico, March 13–17, 2005. P. 359–363.
77. Zhang D., Ramamohanarao K., Versteeg S., Zhang R. Graph Based Strategies to Role Engineering // CSIIRW '10 Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. 2010. Article No. 25.
78. Zukarnain Z.A. Khalid R. Quantum Key Distribution Approach for Cloud Authentication: Enhance Tight Finite Key. International conference on Computer Science and Information Systems (ICSIS'2014) Oct 17-18, 2014 Dubai (UAE). P. 28–33.

THE ANALYSIS OF PROBLEMS OF ACCESS CONTROL ADMINISTRATION IN LARGE-SCALE INFORMATION SYSTEMS

N.F. Bogachenko
Ph.D. (Phys.-Math.), Associate Professor, e-mail: nfbogachenko@mail.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. In the article general questions of access control management for resources of large-scale information systems (LSIS) from positions of formal mathematical models are considered. The properties inherent in LSISs and the requirements imposed on its security policy, which implements the methods and rules of access control, are analyzed. The task is to develop new models, methods and algorithms for managing access control in LSIS.

Keywords: access control, security policy, administration, automation.

Дата поступления в редакцию: 25.05.2018