УДК 004.056.2 004.056.52

А. С. Кубышкин

Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия
E-mail: alexander.kubyshkin@gmail.com

РАЗРАБОТКА МОДЕЛИ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ

Освещен вопрос разграничения прав доступа в автоматизированных системах технологического управления (АСТУ). Рассмотрены основные модели разграничения прав доступа, описаны преимущества и недостатки их применения в АСТУ. Описана комбинированная модель, построенная с учетом специфики АСТУ на принципах мандатной и дискреционной моделей. Приведено доказательство безопасности данной модели, описан механизм ее администрирования.

Ключевые слова: разграничение прав доступа, информационная безопасность, администрирование защиты информации, крупномасштабные распределенные системы.

Введение

Автоматизированные системы технологического управления [1] представляют собой крупномасштабные распределенные системы, предназначенные для ведения учета информации о процессах, которым посвящена система. Учетные данные системы могут быть подвергнуты автоматической обработке для последующего анализа с целью принятия управленческих решений по отношению к управляемым процессам. Таким образом, основным объектом защиты являются учетные данные системы и результаты их обработки.

Приоритетной задачей при рассмотрении АСТУ в части защиты информации является целостность данных. Отсутствие, противоречивость или недостоверность данных лишает смысла использование системы. Стоимость восстановления потерянных или модифицированных данных обычно значительно превышает убытки от их раскрытия. На втором месте по приоритету стоит конфиденциальность. Для АСТУ недопустимо раскрытие информации о стратегических объектах, коммерческой информации, персональных данных. Доступность информации в зависимости от технологических процессов, с которыми работает АСТУ, может быть как критичной для технологического управления, так и незначительной. В данной статье не рассматриваются вопросы доступности информации.

Для решения поставленных перед системой защиты задач, согласно требованиям ГОСТа Р 50739-95 «Защита информации от несанкционированного доступа» [2], она должна осуществлять разграничение доступа субъектов к данным, которое производится в соответствии с политикой безопасности. В качестве субъектов выступают активные ресурсы системы, способные воздействовать на объекты, в частности пользователи и программные единицы. Субъекту разрешается оказывать воздействие только при условии успешного прохождения процедур идентификации, аутентификации и авторизации [1]. Идентификация подразумевает регистрацию уникального наименования субъекта. Аутентификация – уста-

[1] Концепция автоматизированной системы технологического управления ОАО «ФСК ЕЭС»: http://www.fsk-ees.ru/media/File/evolution_technology/ASTU_concept.doc?PHPSESSID=1b9cae98037a7f4d7cec2909710c6fa0

[2] ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования / Научно-исследовательский институт «Квант» Главного управления радиопромышленности Комитета по оборонным отраслям промышленности. Введен 09.02.1995, переиздан в апреле 2004 г.

новление подлинности представленных идентификационных данных. Авторизация подразумевает получение прав на требуемый доступ. Идентификация и аутентификация разграничивают субъекты соответственно на идентифицированных / неидентифицированных и аутентифицированных / неаутентифицированных. Идентифицированный субъект допускается только к процессу аутентификации и не может осуществлять запросы к ресурсам системы, что позволено только аутентифицированным субъектам. Детальное разграничение прав доступа осуществляется на этапе авторизации, суть которой заключается в проверке ограничений доступа к объектам, заносимых администратором безопасности. Только авторизованный субъект допускается к функционалу системы и к хранимым в ней данным.

Ограничения должны осуществляться по следующим признакам:

- роль субъекта;
- домен безопасности субъекта;
- право доступа к объекту;
- организационная принадлежность субъекта.

Таким образом, для получения доступа субъект должен подать системе защиты запрос, включающий идентификатор субъекта, аутентификационные параметры и содержание запроса.

Важными требованиями к разграничению прав доступа являются удобство администрирования и гибкость настройки политики безопасности. В зависимости от требований в информационных системах реализуют различные модели разграничения прав доступа. В ГОСТе Р 50739-95 говорится о дискреционной и мандатной моделях разграничения прав доступа.

Дискреционная модель разграничения прав доступа

Дискреционная модель представляет собой явно заданные правила доступа субъектов системы к объектам. Такие правила обычно записаны в виде матрицы доступов. Классическая дискреционная модель Харрисона – Руззо – Ульмана (ХРУ) состоит из следующих элементов:

- множество объектов системы *O*;
- множество субъектов системы *S*, подмножество множества *O*;
- множество прав доступа *R* субъектов на объекты. Обычно это права на чтение (*read*), на запись (*write*) или владение (*own*) объектом;
- матрица доступов *M*, строки которой соответствуют субъектам, а столбцы – объектам. Элементами матрицы *M* являются подмножества множества прав доступа.

Функционирование системы рассматривается только с точки зрения изменений в матрице доступов. Возможные изменения определяются набором примитивных операторов [2].

Для произвольных систем ХРУ задача проверки безопасности является алгоритмически неразрешимой. Поэтому дискреционные модели наполняют ограничениями, позволяющими гарантировать безопасность модели.

Чтобы достичь удобства администрирования, в модель включают такие элементы, как роли и группы субъектов, организуют домены безопасности, которые связывают с подмножеством множества объектов наборы допустимых прав. При большом количестве субъектов распространением прав доступа в такой системе управлять сложно. Сужение количества контролируемых объектов происходит за счет возложения ответственности за распространение доступа к объекту на субъект, являющийся владельцем объекта (например, его создателем).

Однако в автоматизированных системах технологического управления такой подход осуществить нельзя. Важным требованием для АСТУ является контроль системы за распространением прав доступа. Это означает, что владельцем всех данных должна выступать сама система и описанное выше решение проблемы администрирования недопустимо. Еще одним фактом в пользу отказа от контроля доступа объектов субъектом-владельцем является возникновение уязвимости, связанной с атакой троянским конем.

Мандатная модель разграничения прав доступа

Мандатная модель управления доступом основана на правилах секретного документооборота, принятых в государственных и правительственных учреждениях многих стран. Всем объектам и субъектам в системе назначаются метки конфиденциальности. Контроль доступа осуществляется на основании двух правил:

- субъект имеет доступ на чтение только тех объектов, чей уровень конфиденциальности не выше его;
- субъект имеет доступ на запись только в те объекты, чей уровень конфиденциальности не ниже его.

Задача мандатной модели в том, чтобы не допустить информационные потоки от объектов с более высоким уровнем конфиденциальности к объектам с более низким уровнем конфиденциальности. Мандатные модели обычно рассматривают на примере классической модели Белла – ЛаПадулы. Основными элементами этой модели являются:

- множество объектов системы *O*;
- множество субъектов системы *S*, подмножество множества *O*;
- множество прав доступа *R* субъектов на объекты. Оно состоит из двух элементов: право на чтение (*read*) и права на запись (*write*);
- матрица доступов *M*, строки которой соответствуют субъектам, а столбцы – объектам. Элементами матрицы M являются подмножества множества прав доступа;
- решетка *C* уровней конфиденциальности;
- функция *F*, отображающая множество объектов в уровни конфиденциальности.

К системе в процессе ее функционирования осуществляются запросы на изменение матрицы доступов и функции *F*. Результатом изменения является переход системы из одного состояния в другое. Состояние называется безопасным тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности субъекта доминирует над уровнем безопасности объекта и когда для каждого субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности объекта доминирует над уровнем безопасности субъекта [2]. Для мандатной модели разграничения прав доступа Белла – ЛаПадулы имеет место критерий безопасности. Система безопасна тогда и только тогда, когда ее начальное состояние безопасно и все состояния, достижимые из начального путем применения конечной последовательности запросов к системе, безопасны. Выполнение этого критерия гарантирует теорема безопасности мандатной модели. Система безопасна тогда и только тогда, когда начальное состояние безопасно и осуществляется контроль доступа на основании двух приведенных выше правил.

Применение такой модели дает ряд преимуществ. Во-первых, контроль над распространением прав доступа осуществляется самой системой, следовательно, все данные системы принадлежат ей, а не конкретным пользователям. Во-вторых, администрирование в системе сводится к указанию уровня конфиденциальности, не надо следить за исполняемыми функциями (их всего две: чтение и запись). В-третьих, мандатная модель исключает проблему троянских коней. В случае отсутствия права «execute» на передачу управления другим программам это очевидно, в общем случае это происходит благодаря наличию уровней конфиденциальности и правил доступа.

Однако, имея дело с АСТУ, возникает ряд сложностей, препятствующих использованию мандатной модели разграничения прав доступа. Порожденная определенной спецификой предметной области мандатная политика безопасности основывается на уровнях безопасности, которые априори существуют в предметной области. АСТУ изначально не предполагает наличия подобных ограничений, поэтому их надо либо вводить искусственно, либо отказаться от модели. Также в классической модели присутствует только два права доступа – чтение и запись, которых недостаточно для моделирования сложных процессов технологического управления.

Комбинированная модель

Мы рассмотрели наиболее популярные модели разграничения прав доступа, показав их преимущества и недостатки для использования в АСТУ. Для того чтобы избежать ограничений и недостатков перечисленных решений, предлагается использовать модель, представляющую собой комбинацию принципов мандатной и дискреционной моделей.

Прежде чем приступить к описанию комбинированной модели, сделаем небольшое отступление в предметную область. АСТУ являются многоцелевыми системами, объединенными в один класс, поскольку они решают схожий набор типовых задач, связанных со сбором и хранением данных, с их ручным вводом и модификацией, экспортом и импортом, расчетом учетных показателей, визуализацией данных, генерацией отчетов и документооборотом. Все эти действия производятся над основными типами объектов, с которыми работают подобные системы:

- элементы организационной структуры;
- производственные объекты;
- производственные ресурсы;
- документы;
- события;
- результаты измерений.

В зависимости от предметной области типы объектов могут либо появляться, либо иметь различную интерпретацию. Например, производственным ресурсом может считаться как оборудование, используемое в технологическом процессе, так и персонал, который этот процесс обслуживает. В области энергетики важным понятием являются точки учета – это точки линии электропередач, в которых происходит расчет учетных показателей, а также учетные показатели, которые представляют собой совокупности таких точек. В рамках вопроса информационной безопасности все эти объекты являются объектами защиты. Субъектами в данном случае выступают пользователи системы.

Формальное описание комбинированной модели. За основу комбинированной модели возьмем дискреционную модель с типизированной матрицей доступов (ТМД) [2] и изменим ее в соответствии с принципами мандатной модели. ТМД включает следующие элементы:

- множество объектов системы O;
- множество субъектов системы S, подмножество множества O;
- множество прав доступа R субъектов на объекты;
- матрица доступов M и ее начальное состояние. Строки матрицы соответствуют субъектам, а столбцы – объектам. Элементами матрицы M являются подмножества множества прав доступа;
- множество типов T;
- множество команд C, включающих условия выполнения и интерпретацию в терминах элементарных операций;
- функция t, которая отображает множество объектов во множество типов.

Состояние системы описывается четверкой S, O, M, t. Переход между состояниями осуществляется с помощью команд из множества C. Перед выполнением команды происходит проверка типов фактических параметров. Если они не совпадают с указанными в определении, то команда не выполнится. В таблице приведен набор примитивных операторов, который содержит модель с типизированной матрицей доступов. Здесь не используется удаление, так как в АСТУ все объекты связаны с журналом событий и не удаляются. Типизированная модель является обобщением модели ХРУ, которую можно рассматривать как частный случай ТМД с одним типом для всех объектов и субъектов. С другой стороны, любую систему ТМД можно представить через систему ХРУ, введя для обозначения типов специальные права доступов, а проверку типов в командах заменив проверкой наличия соответствующего права доступа. Так, модель ТМД дает все преимущества и недостатки, которые имеет модель ХРУ, но к тому же позволяет работать с разнотипными объектами. Для АСТУ типами могут выступать типы самих объектов защиты, т. е. T = {*Элемент организационной структуры*, *Производственный объект*, *Событие, Документ*, *Ресурс*, *Измерение, Пользователь*}.

Примитивные операторы модели ТМД

Примитивный оператор	Исходное состояние $q = (S, O, M)$	Результирующее состояние $q' = (S', O', M')$
«Внести» право r в $M[s, o]$	$s \in S$ $o \in O$	$S' = S,\ O' = O,\ t'(o) = t(o),$ для $o \in O,\quad M[s,o] = M[s,o] \cup \{r\},$ для $(s', o') \neq (s, o)$ справедливо равенство $M[s,o] = M[s,o]$
«Удалить» право r из $M[s, o]$	$s \in S$ $o \in O$	$S' = S,\ O' = O,\ t'(o) = t(o),$ для $o \in O,\quad M'[s,o] = M[s,o] / \{r\},$ для $(s', o') \neq (s, o)$ справедливо равенство $M'[s', o'] = M[s', o']$
«Создать» субъект s с типом t_s	$s' \notin O$	$S' = S \cup \{s'\},\quad O' = O \cup \{s'\},$ для $o \in O$ справедливы равенства $t'(o) = t(o),\quad t'(s') = t_s,$ для $(s, o) \in S \times O$ справедливо равенство $M'[s,o] = M[s,o],$ для $o \in O'$ справедливо равенство $M'[s', o] \in Ø,$ для $s \in S'$ справедливо равенство $M'[s, s'] \in Ø$
«Создать» объект o с типом t_o	$o' \notin O$	$S' = S,\ O' = O \cup \{o'\},\ t'(o') = t_o,$ для $(s, o) \in S \times O$ справедливо равенство $M'[s,o] = M[s,o]$, для $s \in S'$ справедливо равенство $M'[s, o'] \in Ø$

Для компенсации недостатков, наследованных вместе с моделью ХРУ, мы позаимствуем принципы мандатной модели разграничения прав доступа. Рассредоточения управления доступами можно избежать, воспользовавшись принципом, согласно которому все данные системы принадлежат системе и она осуществляет контроль над распространением прав доступа. Для этого мы исключим из множества прав доступа право владения объектом «*own*». Также, чтобы избежать угрозы, связанной с атакой троянским конем, мы исключим право «*execute*» из множества прав доступа. Предоставим системе самой решать, в каких строго регламентированных случаях передача управления должна иметь место.

Теперь, когда дано описание комбинированной модели для АСТУ, перейдем к доказательству теоремы безопасности.

Безопасность комбинированной модели. Для комбинированной модели воспользуемся следующим критерием безопасности: если начальное состояние системы безопасно и все переходы системы из состояния в состояние безопасны, то система безопасна. Покажем, что теорема безопасности, сформулированная для классической дискреционной модели, удовлетворяет предложенному критерию, а комбинированная модель в свою очередь удовлетворяет условиям теоремы для классической дискреционной модели. Важным понятием, которым мы воспользуемся, будет понятие монооперационной модели [2].

Определение: монооперационная модель – модель, в которой все команды содержат не более одного примитивного оператора.

Определение: в результате выполнения команды $c(x_1, \ldots, x_k)$ возможна утечка права r, если при переходе системы из состояния q_0 в состояние q_1 через команду c выполняется примитивный оператор, вносящий право r в элемент матрицы доступов M, до этого r не содержащий.

Определение: начальное состояние системы q_0 безопасно по отношению к некоторому праву r, если невозможен переход системы в такое состояние q_1, в котором возможна утечка права r.

Теорема: для монооперационной классической дискреционной модели существует алгоритм, проверяющий, является ли начальное состояние системы безопасным по отношению к праву r.

Если начальное состояние безопасно, то это означает, что оно безопасно по отношению к каждому праву из множества прав доступа. Также это означает, что для всех возможных последовательностей команд для безопасного начального состояния не существует команды, которая перевела бы систему в небезопасное состояние. Поэтому теорема полностью соответствует предложенному критерию. Нас будет интересовать следствие из теоремы.

Следствие: комбинированная модель является безопасной.

Доказательство: покажем, что все команды комбинированной модели можно представить в виде эквивалентного набора монооперационных команд. Команда наделения субъекта правами доступа представима набором монооперационных команд, вносящих последовательно по одному праву доступа для субъекта. Команда создания объекта выполняется в два этапа. На первом происходит непосредственно создание объекта субъектом – это по определению монооперационная команда. На втором этапе система наделяет субъект правами доступа к объекту. Как было показано выше, наделение представляет собой команду, эквивалентную набору монооперационных команд. Команды удаления объекта в АСТУ не предусматриваются, что уже было отмечено раньше. Команды модификации объектов и прочие команды не содержат примитивных операторов и не рассматриваются в рамках вопроса разграничения прав доступа. Следовательно, комбинированная модель удовлетворяет условиям теоремы и является безопасной.

В автоматизированных системах технологического управления разрешение доступа к какому-нибудь объекту может полностью определяться расположением объекта в том или ином производственном объекте и правами доступа субъекта к этому производственному объекту. В данном случае объект доступа может рассматриваться не как самостоятельный объект защиты, а как часть другого объекта защиты – производственного объекта. Поэтому мы можем рассматривать команды создания такого объекта и внесения прав доступа к нему, полностью повторяющие права доступа на производственный объект, как команды модификации производственного объекта, а следовательно, не рассматривать вообще, так как команды модификации объектов не рассматриваются в рамках вопроса разграничения прав доступа.

Администрирование комбинированной модели. Администрирование систем безопасности является важным вопросом в осуществлении контроля безопасности. Количество объектов и субъектов в АСТУ велико, и администратору сложно работать с матрицей доступов напрямую. Для упрощения администрирования используют различные механизмы администрирования.

Традиционным механизмом является механизм ролей. Роли представляют собой множества прав доступа, каждое из которых соответствует некоторому бизнес-процессу, моделируемому системой. Подобно должностям на предприятии роли часто образуют иерархию с отношением включения одной роли в другую, как включения одного множества прав доступа в другое. В данной работе не рассматриваются административные роли и модификация иерархии ролей. К тому же во многих случаях можно пренебречь этой функциональностью для АСТУ. Это связано с тем, что потребители АСТУ – крупные предприятия, уже многие годы существующие на рынке. В таких структурах все технологические процессы уже налажены, поэтому достаточно воспользоваться фиксированным набором пользовательских ролей.

Пользователь, наделенный ролью, имеет права доступа в соответствии с ролью ко всем данным в системе. Это недопустимо в большой корпоративной среде. Чтобы избежать несанкционированного доступа, на данных вводятся различные структуры. В общем случае это частичный порядок. Отображение объектов защиты в этот частичный порядок разбивает данные на домены, доступные разным пользователям. Обычно под доменом понимают набор объектов и прав доступа к каждому объекту.

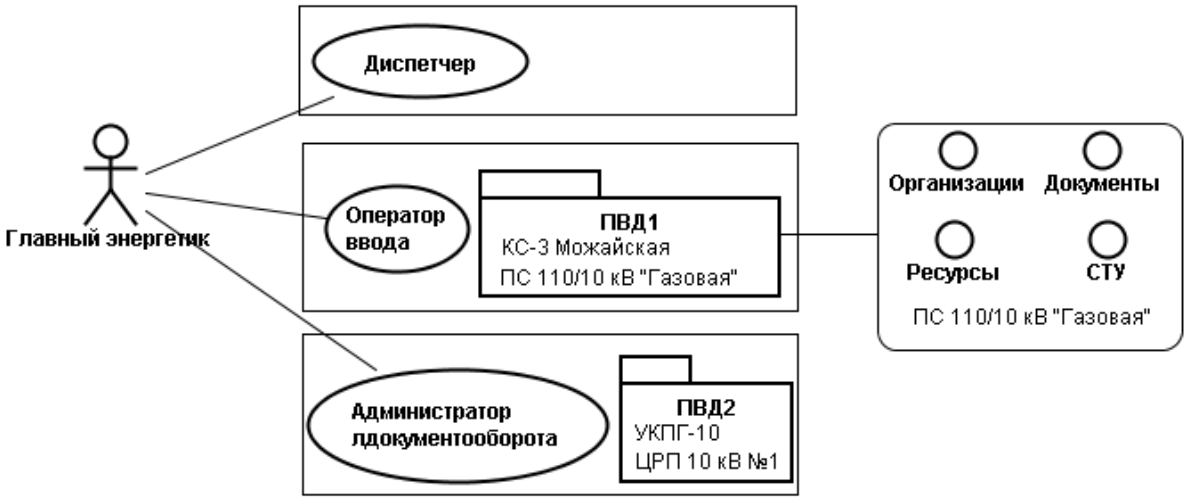

Рис. 1. Пример получения пользователем права доступа к ресурсу системы

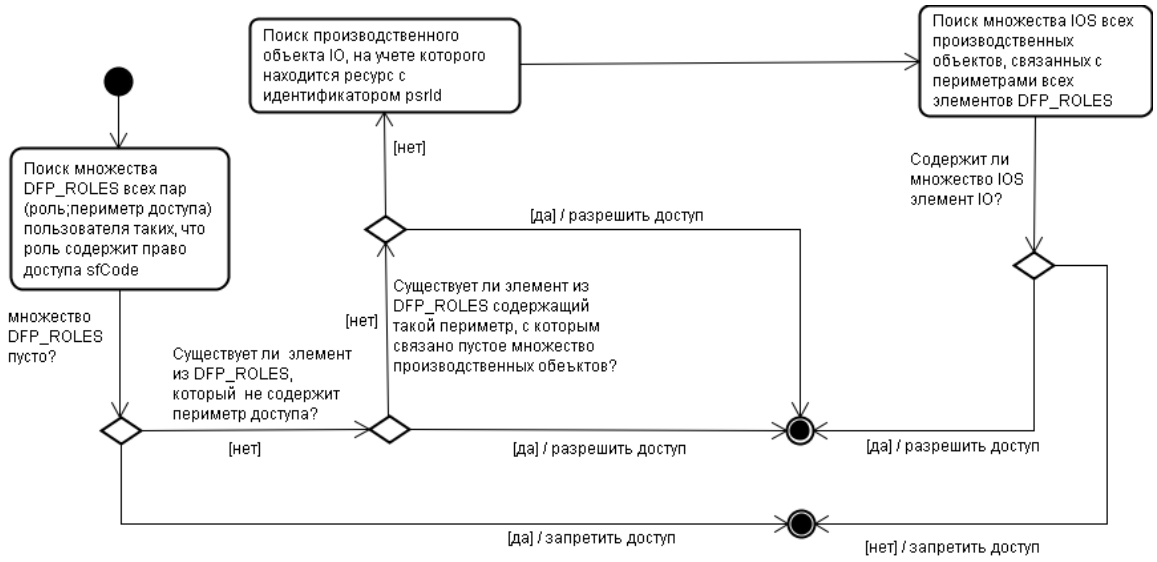

Рис. 2. Алгоритм получения прав доступа к объекту

Жесткая связь объектов с правами доступа лишает гибкости и удобства администрирования. Но в соответствии с RFC 2196 [3] должна обеспечиваться гибкость настройки политики безопасности, в том числе для АСТУ в части разграничения прав доступа к данным технологического учета и результатам их обработки. Предлагается полностью отделить эти понятия. Множества прав доступа будут задаваться ролями, а множества объектов будут формировать профиль выборки данных (ПВД). Такое разделение позволит повторно использовать домен с другими правами доступа. Матрица прав доступа тогда будет задаваться тройками (субъект, роль, ПВД). Недостатком такого подхода является сложность установления права доступа к каждому объекту из ПВД. Однако АСТУ работает с большим количеством объектов и столь детальное разграничение прав доступа не требуется. Детализации на уровне типов

[3] RFC 2196 – Site security handbook // B. Fraser [SEI/CMU]. September 1997.

объектов достаточно, а это гарантируется типизированной матрицей доступов. Таким образом, мы отказываемся от ненужной гибкости и получаем ее там, где необходимо.

Пример получения доступа. Посмотрим, как осуществляется получение прав доступа к объекту на выполнение с ним некоторого действия (рис. 1).

Пользователь, находящийся на должности главного энергетика, обладает ролями «Диспетчер», «Оператор ввода», «Администратор документооборота». С ролями «Оператор ввода» и «Администратор документооборота» связаны профили выборки данных ПВД1 и ПВД2 соответственно. Предположим, что главный энергетик обратился к системе, чтобы получить некоторое право доступа к ресурсу из производственного объекта ПС 110/10 кВ «Газовая». Система проверяет, есть ли среди ролей пользователя та, что содержит запрашиваемое право доступа. Пусть «Оператор ввода» – это нужная нам роль. С ней связан профиль выборки данных ПВД1. Если запрашиваемый ресурс содержится в ПВД1, то система разрешает пользователю доступ к ресурсу, в противном случае доступ запрещается.

Данный алгоритм разрешения запроса пользователя на получение права доступа к ресурсу системы показан на рис. 2.

Результаты работы

Для использования в крупномасштабных распределенных системах класса АСТУ была сформулирована комбинированная модель разграничения прав доступа. Для модели была доказана теорема безопасности, гарантирующая наличие алгоритма проверки безопасности начального состояния системы. Также был разработан механизм администрирования системы безопасности, позволяющий удобно и гибко работать с правами доступа в АСТУ. Описанные в данной работе комбинированная модель и механизм ее администрирования были реализованы в виде программного модуля защиты информации интеграционной платформы учета и управления энергообеспечением «Энергиус». Модуль защиты информации был успешно внедрен в систему «Оперативные заявки» на объектах ООО «Газпром энерго».

Список литературы

1. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника, 2004. 384 с.

2. *Девянин П. Н.* Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Академия, 2005.

Материал поступил в редколлегию 15.06.2010

A. S. Kubyshkin

DESIGNING ACCESS CONTROL MODEL FOR AUTOMATED TECHNOLOGICAL PROCESS MANAGEMENT SYSTEMS

This paper discusses problem of access control for technological process management systems. The author of the paper looks over pros and cons of basic access control models as applied to the mentioned class of systems. The author gives the definition for combined access control model, based on the both mandatory and discretionary access control models in consideration of technological process management systems. The author also gives theorem proving of security model and describes security administration mechanism.

Keywords: mandatory access control, discretionary access control, information security managing, large-scale distributed systems.