Уфа : УГАТУ, 2009 Вестник УГАТУ • Управление, ВТ и И Т. 12, № 1(30). С. 218–225

УДК 004.056.52

Д. В. КИРИЛЛОВ

ОСНОВНЫЕ ПРИНЦИПЫ СОБЫТИЙНО-ОБУСЛОВЛЕННОГО ДЕЛЕГИРОВАНИЯ И ОТЗЫВА ПОЛНОМОЧИЙ В СИСТЕМАХ КОНТРОЛЯ ДОСТУПА НА ОСНОВЕ РОЛЕЙ

В работе рассматриваются базовые принципы событийно-обусловленного делегирования полномочий (СОДОП), основные компоненты модели СОДОП, описываются алгоритмы выполнения основных операций. *Делегирование полномочий ; контроль доступа на основе ролей ; алгоритмы операций делегирования полномочий ; управление КДОР*

В основе контроля доступа на основе ролей (КДОР) лежит понятие роли, которая представляет собой некоторую абстракцию должности в контексте организационной структуры и обладает соответствующим набором привилегий. Таким образом, в КДОР полномочия на выполнение тех или иных операций назначаются администратором системы не конкретному пользователю системы, а роли. Пользователь, таким образом, получает привилегии на выполнение тех или иных операций путем ассоциирования его с той или иной ролью.

Особенностью КДОР является то, что владельцем любого объекта системы, независимо от того, кем он создан, является организация, а не непосредственный создатель объекта. Таким образом, любые операции по разрешению доступа к тому или иному объекту (выполнению операции) выполняет администратор системы.

Эта особенность модели КДОР, с одной стороны, позволяет реализовывать в достаточной степени надежные и управляемые с точки зрения безопасности системы. Однако существуют и очевидные минусы: сложность администрирования системы, ее недостаточная гибкость и «время отклика» (то есть непосредственное выполнение процедуры назначения той или иной операции роли) на организационные решения.

Частично данные проблемы решает принцип делегирования полномочий, в соответствии с которым пользователю разрешается передавать (временно или постоянно) другому пользователю часть или все полномочия из множества назначенных ему.

Использование делегирования полномочий делает систему КДОР более удобной, но порождает ряд новых проблем:

- высокую вероятность ошибки пользователя в связи с его низкой квалификацией или недостаточным вниманием;
- снижение общего уровня управляемости системы безопасности и, как следствие этого, снижение общего уровня безопасности.

Очевидно, что ни полный контроль со стороны администратора системы, ни классический подход к делегированию полномочий не могут быть признаны идеальным решением описанных проблем, поэтому автором предлагается альтернативный подход к управлению политикой безопасности на основе КДОР – событийно-обусловленное делегирование и отзыв полномочий, далее СОДОП.

Сущностью подхода является то, что процедура делегирования или отзыва полномочий производится в результате некоторого события или последовательности событий, и решение о выполнении процедуры делегирования или отзыва полномочий принимается на основе условий, описывающих некоторое состояние системы. При этом в качестве элементов условия могут использоваться как компоненты КДОР и отношения между ними, так и атрибуты объектов, определяемые на уровне бизнес-логики автоматизированной системы (АС).

Рассмотрим более подробно понятие и основные принципы СОДОП.

Контактная информация: (8927) 294-31-81

1. ОСНОВНЫЕ ПРИНЦИПЫ СОДОП В КОНТЕКСТЕ КДОР

Понятие делегирования полномочий как процесса передачи прав на выполнение некоторого множества операций от одного пользователя другому или от пользователя к некоторой роли, не ассоциированной с пользователем, делегирующим полномочия, в контексте КДОР впервые было рассмотрено в работах Барка, Сандху и др. [2]. Дальнейшие исследования в этом направлении касались либо расширения исходной схемы делегирования полномочий на множество инвариантов модели КДОР [3, 4], либо реализации ограничений делегирования, позволяющих разрабатывать более гибкие в управлении и безопасные с точки зрения предотвращения эскалации прав схемы делегирования полномочий [5, 6, 7].

Другими словами, существующие на сегодняшний момент времени модели делегирования полномочий [3–7] базируются на ряде общих принципов, не выходящих за границы изначальных предпосылок к применению принципов делегирования полномочий, а все изменения направлены исключительно на снижение риска эскалации прав вследствие нарушения некоторых базовых принципов КДОР [1] в результате применения принципов делегирования полномочий [2].

К этим принципам можно отнести следующие:

- субъект, принимающий решение о делегировании полномочий, и субъект, чьи полномочия делегируются, являются одним и тем же субъектом;
- принятие решения о делегировании полномочий и непосредственное выполнение процедуры делегирования полномочий характеризуются незначительной задержкой во времени;
- отзыв ранее делегированных полномочий возможен только 2 способами – либо вручную пользователем, ранее делегировавшим полномочия, или пользователем, наделенным правом назначать и отзывать полномочия (администратором системы), либо автоматически, в результате истечения срока времени действительности делегирования полномочий, определяемого на момент принятия решения о делегировании полномочий.

Данные принципы не позволяют в полной мере реализовать принципы делегирования полномочий, традиционно применяемые в управлении организацией. Поэтому предлагается новая модель делегирования полномочий (СОДОП), которая фактически расширяет существующие модели путем внесения понятия события и связанным с ним автоматическим принятием системой решения о делегировании полномочий. Сформулируем понятие событийно-обусловленного делегирования полномочий следующим образом.

Событийно-обусловленное делегирование и отзыв полномочий – это процесс передачи или отзыва ранее делегированных полномочий от одного пользователя к другому пользователю или роли, не ассоциированной с пользователем, делегирующим полномочия, в результате возникновения некоторого события или последовательности событий в АС и в соответствии с формально описанными условиями делегирования и отзыва полномочий, хранимых в некотором виде в АС.

В отличие от традиционных схем делегирования полномочий [2–7], в СОДОП принятие решения о делегировании полномочий и процедура делегирования полномочий могут быть значительно разнесены во времени, либо в частных случаях процедура делегирования полномочий может не быть выполнена вовсе. Аналогично процедура отзыва полномочий также выполняется в результате наступления некоторого события (в том числе после прохождения некоторого периода времени).

Другое отличие от традиционных подходов к делегированию полномочий заключается в том, что инициатор делегирования полномочий и субъект, чьи полномочия делегируются, в общем случае не являются одним и тем же субъектом. Однако необходимо определить границу применимости данного принципа: он не должен нарушать базовых принципов КДОР и базовых схем делегирования полномочий, выполняющих роль системных ограничений.

Очевидно, что для реализации принципов СОДОП недостаточно имеющихся компонентов и отношений инвариантов моделей КДОР и традиционных схем делегирования полномочий. Поэтому для реализации модели СОДОП необходимо ответить на несколько основных вопросов.

- Какой компонент системы непосредственно выполняет процедуры по делегированию и отзыву полномочий?
- Что понимается под событием в системе?
- Каким образом описываются условия делегирования и отзыва полномочий?
- Каким образом условия делегирования и отзыва полномочий влияют друг на друга?

• Каким образом должно выглядеть поведение системы в результате возникновения того или иного события?

Рассмотрим основные компоненты модели СОДОП, предназначенные для решения поставленных вопросов.

2. ОСНОВНЫЕ КОМПОНЕНТЫ И ОТНОШЕНИЯ СОДОП

Как было сказано выше, модель СОДОП применяется в контексте той или иной инвариантной модели КДОР и одной (или более) базовых моделей делегирования полномочий. Рассмотрим компоненты КДОР и связи между ними, формирующие базовую модель СОДОП, реализуемую на основе «плоского» КДОР и базовой модели делегирования полномочий [2].

К базовым компонентам КДОР, формирующим модель «плоского» КДОР, относятся множества пользователей (USERS), ролей (ROLES), объектов (OBS), операций (OPS), полномочий(PRMS) и сеансов пользователей (SESSIONS).

Пользователь представляет собой абстракцию человека как субъекта системы, однако понятие пользователя может быть расширено и на другие сущности.

Роль представляет собой некоторую абстракцию должности в организации, в контексте информационной системы, наделенную некоторыми полномочиями на выполнение тех или иных операций в системе.

Полномочия – разрешение на выполнение операции над одним или более объектами системы.

Операция – выполнение тех или иных действий в системе.

Взаимосвязь компонентов «плоского» КДОР ($RBAC_0$) представлена на рис. 1. Рассмотрим основные отношения между компонентами системы.

Отношение назначения пользователям ролей (*UA)* – это отношение вида «многие-ко-многим», формально описываемое как:

$$UA \subseteq USERS \times ROLES. \quad (1)$$

Множество полномочий PRMS, представляет собой отношение вида «многие-ко-многим» между элементами множества операций и объектов системы и формально описывается как:

$$PRMS = 2^{OPSxCBS}. \quad (2)$$

Отношение назначения ролям полномочий (PA) представляет собой отношение вида «многие-ко-многим» между элементами множеств полномочий и ролей и формально описывается как:

$$PA \subseteq PRMS \times ROLES. \quad (3)$$

Кроме того, в контексте «плоского» КДОР также определены некоторые функции отображения, связывающие элементы множеств компонентов системы КДОР.

К ним относятся следующие функции:

• assigned_permissions (r: ROLES) → 2^{PRMS}, отображающая некоторую роль *r* на множество разрешений:

$$\text{assigned\_permissions}(r : \text{ROLES}) = \{p \in \text{PRMS} \mid (p, r) \in \text{PA}\}; \quad (4)$$

• Ob (*p*: PRMS) → {op ∈ OPS}, отображающая некоторое разрешение на множество операций и возвращающая некоторое множество операций, связанных с разрешением *p*;

• Ob (*p*: PRMS) → {ob ∈ OBS}, отображающая некоторое разрешение на множество объектов и возвращающая некоторое множество объектов, связанных с разрешением *p*;

• user_sessions(*u:* USERS) → $2^{SESSIONS}$, отображающая некоторого пользователя *u* на множество сеансов, связанных с ним;

• session_roles (*s:* SESSIONS) → $2^{SESSIONS}$, отображающая некоторый сеанс *s* на множество ролей связанных с ним.

• Ob(*p*: PRMS) → {op ∈ OPS}, отображающая некоторое разрешение на множество операций и возвращающая некоторое множество операций, связанных с разрешением *p*.

В базовой модели делегирования полномочий в контексте КДОР ($RBDM_0$), расширяющей модель «плоского» КДОР, путем внесения понятия делегирования пользовательских полномочий определяются дополнительные компоненты и отношения.

В контексте $RBDM_0$ для каждой роли, принадлежащей множеству ROLES, определяется два подмножества назначенных на эту роль пользователей:

• оригинальные пользователи, ассоциированные с ролью Users_O(*r*);

• пользователи, ассоциированные с ролью в результате делегирования полномочий Users_D(*r*).

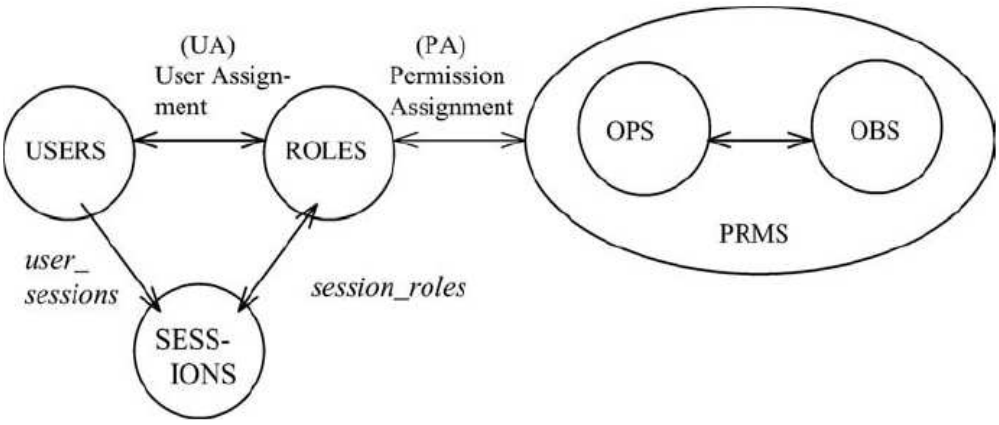

Рис. 1. Компоненты «плоского» КДОР

Соответственно, в дополнение к модели RBAC_0 вводятся следующие отношения:

• отношение UAO вида «многие-ко-многим», связывающее элементы множества ролей и назначенных на эти роли оригинальных пользователей, формально определяемое как:

$$\mathrm{UAO} \subseteq \mathrm{USERS} \times \mathrm{ROLES}. \qquad (5)$$

• отношение *UAD* вида «многие-ко-многим», связывающее элементы множества ролей и назначенных в результате делегирования на эти роли пользователей, формально определяемое как:

$$\mathrm{UAD} \subseteq \mathrm{USERS} \times \mathrm{ROLES}. \qquad (6)$$

Кроме того, в связи с внесением нового типа отношений назначения пользователя на роль, переопределяется отношение назначения пользователей на роль (1) следующим образом:

$$\begin{aligned} &\mathrm{UA} = \mathrm{UAO} \cup \mathrm{UAD} \\ &\mathrm{UAO} \cap \mathrm{UAD} = \varnothing. \end{aligned} \qquad (7)$$

Функции принадлежности оригинальных пользователей к некоторой роли r и пользователей, назначенных на роль в результате делегирования полномочий, формально описываются соответственно:

$$\mathrm{Users\_O}(r) = \{U \mid (U, r) \in \mathrm{UAO}\} \qquad (8)$$

$$\mathrm{Users\_D}(r) = \{U \mid (U, r) \in \mathrm{UAD}\}. \qquad (9)$$

Одним из центральных понятий в контексте RBDM_0 является понятие длительности делегирования полномочий, определяющее для каждой операции делегирование времени, в течение которого делегированные полномочия действительны. Элементы множества длительностей делегирования и элементы множества отношения UAD связываются функцией отображения:

$$\mathrm{Delegate\_roles}: \mathrm{UAD} \to T. \qquad (10)$$

В качестве ограничения на выполнение операции делегирования полномочий выступает отношение can_delegate, определяемое как:

$$\mathrm{can\_delegate} \subseteq \mathrm{ROLES} \times \mathrm{ROLES}. \qquad (11)$$

Например, следующая конструкция: ($a \in$ $\in$ ROLES, $b \in$ ROLES) $\in$ can_delegate, означает, что пользователь, назначенный на некоторую роль a, может делегировать роль a некоторому пользователю, назначенному на роль b.

Отметим, что отношение can_delegate нерефлексивно, что означает недопустимость операции делегирования пользователю, назначенному на ту же роль, на которую назначен делегирующий пользователь и которую этот пользователь делегирует.

Рассмотрим компоненты и отношения, реализующие на базе моделей RBAC_0 и RDBM_0 базовую схему СОДОП.

Как было отмечено выше, в отличие от традиционной схемы делегирования решение о выполнении процедуры делегирования полномочий может принимать субъект отличный от того, чьи полномочия делегируются. Определим субъекта, принимающего решение о выполнении процедуры делегирования или отзыва полномочий, как инициатора делегирования.

Инициатор делегирования – субъект, принимающий решение о делегировании полномочий путем описания условий делегирования.

При этом субъекта (пользователя), чьи полномочия делегируются, назовем делегатором, а субъекта (пользователя или роль), которому делегируются полномочия, назовем делегатом.

В качестве делегата полномочий может выступать любой субъект системы, если выполняются следующие условия:

• не нарушаются системные ограничения используемого инварианта КДОР [1];

• не нарушаются базовые принципы делегирования полномочий [2];

• не нарушается ограничение делегирования (если их присутствие допустимо в контексте выбранной базовой схемы делегирования полномочий), такие как ограничения на переделегирование полномочий [5], ограничения на кросс-делегирование [4].

Таким образом, в наиболее общем виде процесс выполнения операций делегирования полномочий в контексте СОДОП представляет собой описание условий делегирования полномочий инициатором делегирования, уполномоченным на это действие от делегатора полномочий делегату, причем полномочия передаются либо путем ассоциирования с ролью, одновременно назначенной и делегатору полномочий, и инициатору делегирования, либо путем создания так называемой временной роли, наделенной множеством делегируемых полномочий (причем данное множество полномочий также должно быть одновременно назначено инициатору делегирования и делегатору).

Дополнительно к отношениям UAO (5) и UAD (6) определим отношение UAC, связывающее множество инициаторов делегирования, делегаторов и делегатов полномочий, следующим образом:

$$\mathrm{UAC} \subseteq \mathrm{USERS} \times \mathrm{USERS} \times \mathrm{ROLES}. \quad (12)$$

Либо, в соответствии с ранее данными определениями,

$$\mathrm{UAC} \subseteq \mathrm{USERS} \times \mathrm{UAD}. \quad (13)$$

Таким образом, отношение (7) остается без изменений.

В качестве ограничения на отношение делегирования полномочий введем отношение can_init_deleg, формально описываемое следующим образом:

$$\mathrm{can\_init\_deleg} \subseteq (\mathrm{USERS} \cup \mathrm{ROLES}) \times \times \mathrm{ROLES} \times \mathrm{ROLES}. \quad (14)$$

Отношение can_init_delegation означает, что некоторый пользователь или пользователь некоторой роли, являющийся инициатором делегирования, может инициировать делегирование членства в некоторой роли от пользователя также являющимся членом этой роли, пользователю, являющемуся членом другой роли, отличной от делегируемой. Очевидно, что данное отношение можно записать в виде:

$$\mathrm{can\_init\_deleg} \subseteq (\mathrm{USERS} \cup \mathrm{ROLES}) \times \times \mathrm{can\_delegate}. \quad (15)$$

Для того чтобы обеспечить взаимосвязь между компонентами КДОР и компонентам бизнес-логики системы, необходимо иметь некоторые характеристики этих объектов. Для этого введем понятие свойств или атрибутов объектов.

Свойства (атрибуты) объектов – *это* некоторые отличительные характеристики объектов, присущие тому или иному объекту в контексте системы, в котором данный объект присутствует.

Условия делегирования и отзыва полномочий

Условия делегирования и отзыва полномочий (УДОП) являются фундаментальной основой СОДОП и используются для задания точки принятия решения о начале процедуры делегирования полномочий или отзыва полномочий. УДОП задаются с использованием специального языка и правил формальной логики. Фактически УДОП составляются путем объединения событий и свойств некоторых объектов. Если условие истинно, выполняется операция делегирования или отзыва полномочий; если условие ложно, никаких действий не предпринимается.

Решение о выполнении операции делегирования или отзыва полномочий принимается в том случае, если условие имеет значение. В противном случае условие игнорируется до следующего изменения состояния системы.

Механизм событий

Событие – изменение состояние системы, результатом которого стало изменение некоторых свойств компонентов автоматизированной системы, отношений между компонентами системы, а также свойств самой системы. Фактически, любое событие в системе связано с выполнением той или иной операции, причем как в контексте системы разграничения полномочий, так и в рамках АС в целом.

В контексте СОДОП, определим два типа событий:

1) события, связанные с изменением времени;

2) события, связанные с изменением состояния системы.

Определим некоторое состояние системы СОДОП в некоторый момент времени как кортеж:

$$G = \left\langle \begin{matrix} \mathrm{USERS}, \mathrm{ROLES}, \mathrm{OBS}, \\ \mathrm{OBJ\_ATT}, \mathrm{PERMS}, \\ \mathrm{SESSIONS}, \mathrm{UA}, \mathrm{PA} \end{matrix} \right\rangle. \quad (16)$$

В результате выполнения той или иной операции $op \in OPS$ система переходит из состояния G'_{t_0}, что определяется как:

$$G' = \left\langle \begin{matrix} USERS', ROLES', OBS', \\ OBJ\_ATT', PERMS', \\ SESSIONS', UA', PA' \end{matrix} \right\rangle. \quad (17)$$

Определим переход состояния как:

$$G \xrightarrow{op \in OPS} G'. \quad (18)$$

В результате перехода состояния системы вследствие выполнения операции возникает событие. Очевидно, что выполнение любой операции в контексте системы КДОР влечет возникновение события.

С точки зрения СОДОП, любое событие может быть использовано для уведомления монитора делегирования полномочий (МДП) о необходимости инициации делегирования или отзыва полномочий, причем при описании условия не является обязательным привязка к конкретным значением свойств, которые изменяются. Для МДП необходим именно сам факт возникновения события. Однако использование таких непараметрических событий нежелательно, так как обработка их весьма трудоемка.

В общем виде процесс генерации и обработки события, связанного с изменением состояния системы выглядит следующим образом:

1) в результате выполнения операции генерируется уведомление о наступлении события;

2) уведомление поступает в очередь обработки уведомлений МДП;

3) МДП производит последовательную обработку уведомлений доходит до уведомления, сгенерированного в п. 1;

4) осуществляет поиск условий делегирования или отзыва полномочий, в которых имеется привязка к событию, сгенерированному в п. 1;

5) если такие условия найдены, МДП выполняет процедуры делегирования или отзыва полномочий;

6) уведомление удаляется из очереди.

В случае событий, связанных с наступлением определенного времени, механизм обработки событий выглядит несколько иначе. В этом случае за генерацию события отвечает системный таймер, который с заданным интервалом помещает уведомление о наступлении времени в очередь уведомлений МДП. Все остальные шаги аналогичны для событий, связанных с изменением состояния системы.

Правила делегирования полномочий

Правила делегирования полномочий регламентируют порядок выполнения процедур делегирования полномочий с точки зрения их корректности и безопасности.

Правила делегирования и отзыва полномочий – базовые принципы СОДОП, гарантирующие корректность и безопасность выполнения процедур делегирования и отзыва полномочий в соответствии с заданными алгоритмами.

Для того чтобы непосредственно осуществлять выполнение операций делегирования и отзыва полномочий, в системе должен существовать субъект, наделенный правами выступать делегатором полномочий для любого пользователя или роли. В СОДОП таким субъектом является монитор СОДОП.

Монитор СОДОП – специальный субъект системы, отслеживающий события, возникающие в системе, сопоставляющий события в системе с описанными условиями делегирования и отзыва полномочий и выполняющий процедуры делегирования и отзыва полномочий на основе этих условий и в соответствии с правилами СОДОП.

Очевидно, что для внесения монитора СОДОП в модель КДОР необходимо переопределить множество субъектов КДОР следующим образом:

$$S_{\text{СОДОП}} = S \cup \{\text{d\_monitor}\}. \quad (19)$$

В качестве остальных компонентов модели СОДОП и ее инвариантов выступают компоненты тех инвариантов моделей КДОР и базовых схем делегирования полномочий, в контексте которых применяется модель СОДОП.

Исходя из приведенного формального описания СОДОП, рассмотрим несколько алгоритмов базовых операций СОДОП.

3. БАЗОВЫЕ АЛГОРИТМЫ СОДОП

К базовым алгоритмам модели СОДОП относятся внесение условий делегирования и отзыва полномочий и выполнение операций по делегированию и отзыву ранее делегированных полномочий. Рассмотрим алгоритмы выполнения этих операций.

Внесение условий делегирования / отзыва полномочий.

При внесении нового условия делегирования или отзыва полномочий выполняется следующая последовательность действий:

- проверка корректности и непротиворечивости условия;

• проверка достижимости состояния системы в результате возникновения цепочки событий, описанной в условии;

• проверка непротиворечивости вновь вносимого условия ранее описанным условиям;

• проверка соответствия условия системным ограничениям, ограничениям используемого инварианта КДОР, ограничениям схемы делегирования, ограничениям СОДОП.

Выполнение операции делегирования полномочий

В каждый момент времени τ_i монитор СОДОП находится в ожидании возникновения некоторого события. Пусть произошло некоторое событие $event_1$. В этом случае монитор СОДОП выполняет следующие действия (рис. 1).

1) проход по множеству всех зарегистрированных в системе условий СОДОП и выбор из них тех, для которых событие $event_1$ является ожидаемым для делегирования полномочий;

2) для каждого найденного условия событие $event_1$ выталкивается из цепочки ожидаемых событий;

3) после того, как событие вытолкнуто, определяется длина цепочки ожидаемых событий;

4) если длина цепочка событий не равна нулю, то происходит переход к следующему условию;

5) если длина цепочки равна 0, то происходит вычисление выражения условия делегирования;

6) если вычисленное значение равно «ЛОЖЬ», то происходит переход к следующему условию;

7) если вычисленное значение равно «ИСТИНА», производится переход к блоку проверки ограничений;

8) последовательно выполняется проверка системных ограничений, ограничений инварианта КДОР, ограничений схемы делегирования, ограничений СОДОП;

9) если хотя бы один из видов ограничений нарушено, то происходит переход к следующему условию СОДОП;

10) если ни одно из ограничений не нарушено, то выполняется операция делегирования полномочий в соответствии с определенными правилами делегирования полномочий.

Отметим важную особенность алгоритма: так как операция делегирования полномочий порождает изменение состояния системы, то система генерирует новые события, помещая в очередь событий, поэтому выполнение соответствующей операции может привести к значительным изменениям состояния системы. Поэтому в контексте СОДОП серьезную роль играют правила и ограничения, которые выполняют в том числе и стабилизирующую функцию, предотвращая неконтролируемое поведение системы.

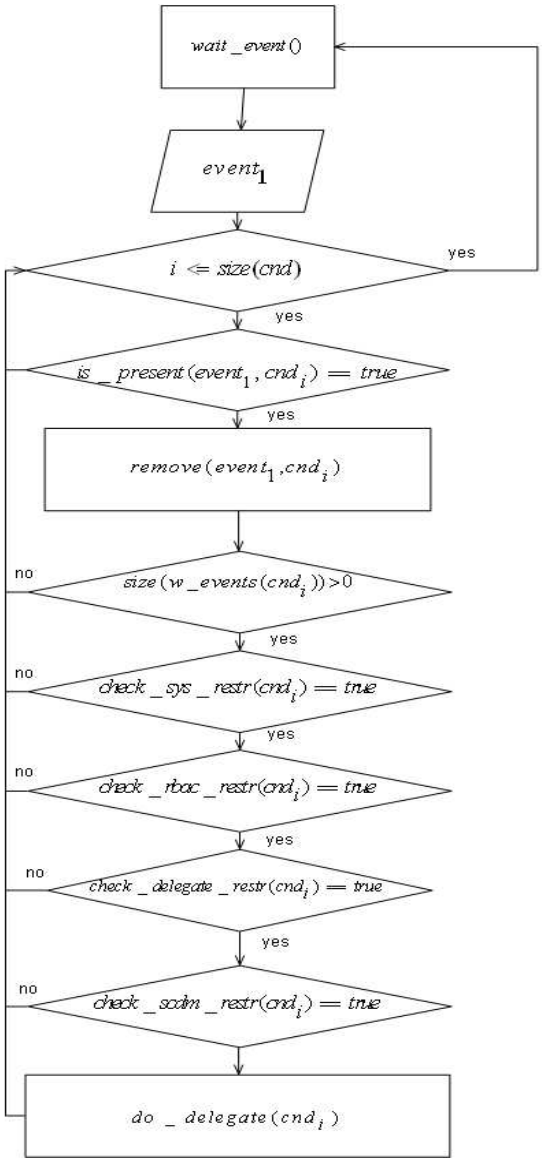

Рис. 2. Блок-схема алгоритма выполнения операции делегирования в СОДОП

Выполнение операции отзыва полномочий

При выполнении операции отзыва делегированных полномочий последовательность шагов аналогична последовательности шагов при выполнении операции делегирования полномочий, с той разницей, что при проходе по списку условий, среди них отбираются те, в которых в качестве выполняемой операции указан отзыв полномочий. Кроме того, после завершения

операции отзыва полномочий условие отзыва уничтожается.

Очевидно, что описанные алгоритмы являются весьма обобщенными, так как в них не учитываются особенности реальных систем, в которых они применяются. Например, в 8-м шаге алгоритма выполнения операции делегирования полномочий может отсутствовать проверка выполнения тех или иных ограничений в случае, если в используемом инварианте КДОР или базовой модели делегирования полномочий эти ограничения отсутствуют.

Также необходимо отметить, что в реальных условиях алгоритм выполнения операции отзыва полномочий принимает значительно более сложный вид, так как в приведенном алгоритме не учитываются случаи циклически выполняемых условий.

ЗАКЛЮЧЕНИЕ

Предложенная модель СОДОП позволит решить ряд задач, среди которых:

- сокращение нагрузки на администратора безопасности – в контексте СОДОП основной задачей администратора системы фактически станет конфигурирование системы путем связывания событий и объектов подсистемы безопасности и подсистемы бизнес-логики правилами СОДОП, а не постоянный контроль за изменениями в организационной структуре;
- появление возможности отложить решение о делегировании полномочий до возникновения определенного события, описанного в условии делегирования или отзыва полномочий (реализация принципа исполнения обязанностей);
- увеличение общей гибкости системы за счет большей степени связанности уровней безопасности и бизнес-логики;
- ошибки в назначении привилегий вероятны только в случае неправильности принципов управления и разделения обязанностей в системе, но не в результате неправильных действий администратора безопасности или пользователя.

Указанные преимущества модели СОДОП перед традиционными схемами делегирования полномочий говорят о широких перспективах использования ее в практических целях.

СПИСОК ЛИТЕРАТУРЫ

1. **Sandhu, R.** Role-based access control models / R. Sandhu, E. Coyne, H. Feinstein, C. Youman // IEEE Computer. 1996. № 29(2). P. 38–47.

2. **Barka, E.** A role-based delegation model and some extensions / E. Barka, R. Sandhu // Proc. of 16th Annual Computer Security Applications Conference(ACSAC'00). 2000. P. 168–177.

3. **JongSoon, P.** A role-based delegation model using role hierarchy supporting restricted permission inheritance / P. JongSoon, L. YoungLok, L. HyungHyo, N. BongNam // Proc. of the International Conference on Security and Management, CSREA Press, 2003. P. 294–302.

4. **Tamassia, R.** Role-based cascaded delegation / R. Tamassia, D. Yao, W.H. Winsborough // Proc. of the 9th ACM Symposium on Access Control Models and Technologies, ACM, 2004. P. 146–155

5. **Zhang, L.** A rule-based framework for role-based delegation and revocation / L. Zhang, G.-J. Ahn, B.-T. Chu // ACM Trans.Inf.Syst.Secur. 2003. № 6(3). P. 404–441.

6. **Zhang, X.** PBDM: A flexible delegation model in RBAC / X. Zhang, S.Oh, R. Sandhu // Proc. of the 8th ACM symposium on Access control models and technologies, ACM Press, 2003. P. 149–157.

7. **Gollmann, D.** Delegation in role-based access control / D. Gollmann, J. Meier, A. Sabelfeld // ESORICS 2006, LNCS 4189. 2006. P. 174–191.

ОБ АВТОРЕ

Кириллов Денис Викторович, ст. преп. каф. БИС САМГУ. Дипл. спец. по организации и технологии защиты информации (САМГУ, 2005). Иссл. в обл. моделей контроля доступа на основе ролей, делегирования полномочий, систем автоматизации упр-я в высш. учеб. заведениях.