УДК 681.3

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПОЛИТИКИ БЕЗОПАСНОСТИ ЭТАЛОННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА ОСНОВЕ ЭМЗАС-СЕТИ

А. С. Дубровин[1], В. И. Сумин[2], М. В. Коротков[3], А. Ю. Немченко[3]

[1]Воронежская государственная технологическая академия
[2]Воронежский институт МВД РФ
[3]5 центральный научно-исследовательский испытательный институт МО РФ

Построена на основе аппарата ЭМЗАС-сетей математическая модель политики безопасности (ПБ) эталонной автоматизированной системы (АС) в смысле эталонной модели защищенной автоматизированной системы (ЭМЗАС). Построенная модель дает математическое основание для формулирования, изучения и реализации ПБ эталонной АС, что создает существенные теоретические предпосылки для реализации концепции эталонной АС в смысле ЭМЗАС в практике разработки АС критического применения.

ВВЕДЕНИЕ

Для унификации архитектурного облика автоматизированных систем (АС) критического применения (КП) за счет стандартизации интерфейсов сопряжения прикладных процессов с уровневыми комплексами сервисов безопасности на основе их декомпозиции по уровням доступа к ресурсам АС была предложена концепция эталонной АС в смысле 15-уровневой эталонной модели защищенной автоматизированной системы (ЭМЗАС) [1]. Модель эталонной АС призвана служить идеализированной моделью АС, реализующей принципиально безопасную технологию циркуляции информации. В целях моделирования эталонных АС необходимо создание подходящей проблемно-ориентированной теории. Для этого на базе известных Е-сетевых формализмов [2], возникших в развитие сетей Петри, в [3] предложен новый аппарат математического моделирования — ЭМЗАС-сети, эквивалентные Е-сетям специального вида. На основе проведенного исследования на предмет выразительности ЭМЗАС-сетей, в частности, в сравнении с общеизвестными сетевыми моделями, выявлен ряд их замечательных свойств. Их структура в высокой степени регулярна, за счет чего пространство состояний всей совокупности гиперпроцессов эталонной АС представляется в ЭМЗАС-сети относительно просто, а политика безопасности (ПБ) на ней — относительно прозрачно. Найдено подходящее специфическое синтаксическое представление ЭМЗАС-сетей на основе минимизации описательных средств (каноническая форма сети) — граф особого вида, вершинами которого являются модули, содержащие позиции. Структура сети блочная, динамика определяется перемещением по заданным процедурам (преобразования, разрешающим и временной задержки) объектов (фишек), группирующихся в транзакты. Введение аппарата ЭМЗАС-сетей открывает путь для систематического исследования их математических свойств как инструмента разработки АС КП на основе концепции эталонной АС в смысле ЭМЗАС. Как очередной шаг в этом направлении, целью данной статьи является построение на основе аппарата ЭМЗАС-сетей математической модели ПБ эталонной АС в смысле ЭМЗАС (определение ПБ на ЭМЗАС-сети).

Концепция эталонной АС в смысле ЭМЗАС предполагает проведение не произвольных ПБ, а присущего именно ей класса ПБ, в содержательном плане предложенного в [4]. Именно такие ПБ являются в данной статье объектом математического моделирования. ПБ эталонной АС соединяет удобство и естественность дискреционной моде-

ли с доказательностью моделей конечных состояний, являясь моделью конечных состояний по существу и моделью дискреционного доступа по форме. Тогда при задании глобальной ПБ в форме дискреционных полномочий доступа выполнение гарантирующей ее локальной ПБ обеспечивается автоматически с использованием механизма задания требований к субъектному наполнению эталонной АС при организации изолированной программной среды (ИПС). Тем самым, концепция эталонной АС есть развитие концепции ИПС [5], лежащей в основе методологии гарантирования защиты АС и являющейся расширением зарубежных подходов к реализации ядра безопасности в направлении учета контроля порождения субъектов.

При описании локальной ПБ многоуровневого доступа к ресурсам посредством цепочки авторизованных доступов между субъектами разных уровней (что характерно для ЭМЗАС) необходимо задавать правила безопасного межсубъектного взаимодействия в эталонной АС. Тогда если начальное состояние АС безопасно, и все межсубъектные взаимодействия не нарушают ограничений, сформулированных локальной ПБ (локальных ограничений), то любое состояние АС безопасно.

Правила межсубъектного взаимодействия не просто дополняют правила разграничения доступа субъектов к объектам, а обобщают их за счет взгляда на межсубъектные взаимодействия с точки зрения, близкой категориям объектно-ориентированного программирования, интегрирующей данные с обрабатывающими их процедурами и, тем самым, объекты с соответствующими субъектами. При этом доступ субъектов к объектам реализуется вызовом с соответствующими параметрами необходимых методов других субъектов (более низкого уровня) [4].

Как основу для математического моделирования ПБ эталонной АС выберем *ЭМЗАС-сеть в канонической форме*. Каждый *модуль ЭМЗАС-сети* относится к одному из 13 нижних уровней ЭМЗАС, идентифицируется своим индексом и содержит набор пар противолежащих входных и выходных позиций. Все входные позиции простые, а все выходные — разрешающие. Пары противолежащих позиций одного модуля различаются между собой своей авторизацией, причем для каждой авторизации существует единственная пара противолежащих позиций. Если число авторизаций в ЭМЗАС-сети обозначить через N, то любой модуль содержит N входных позиций и N выходных. Каждая пара противолежащих позиций с номером авторизации α модуля с индексом I характеризуется булевозначным *признаком допустимости авторизации* $r = r(I,\alpha)$, показывающим, может ли в эталонной АС быть инициирован из соответствующего модуля процесс с данной авторизацией.

Для идентификации модулей и блоков ЭМЗАС-сети используется механизм их индексации индексами различного порядка. Индекс произвольного j-го порядка определяется как выражение следующего вида: $i_1.i_2.....i_j$, представляющее собой последовательность j натуральных чисел, записанных через точку. В основе индексации лежит отнесенность модулей уровням ЭМЗАС и нумерация модулей в содержащем их блоке. Модули l-го уровня ЭМЗАС индексируются индексами порядка $(13-l)$, $l = \overline{1,L}$, где L — число уровней ЭМЗАС-сети (15-уровневой ЭМЗАС соответствует $L = 13$). Все модули данного блока делятся на верхние и нижние (относящиеся к более высокому и более низкому уровню ЭМЗАС соответственно). Любой *блок ЭМЗАС-сети* с некоторым индексом I содержит единственный верхний модуль (№ 0 в блоке) и $K[I]$ нижних модулей (с номерами от 1 до $K[I]$ в блоке). Индекс блока совпадает с индексом его верхнего модуля. Индекс нижнего модуля с номером $j = \overline{1,K[I]}$ в блоке с индексом I определяется как $I.j$.

Объекты (фишки) могут обладать набором признаков (атрибутов). С каждой позицией ассоциированы процедура временной задержки и процедура преобразования. С каждой разрешающей позицией ассоциирована разрешающая процедура, позволяющая организовывать условные ветвления и переключения при перемещении объектов. Динамика ЭМЗАС-сети в канонической форме определяется перемещением объектов из одних позиций в другие, что формально эквивалентно изменению маркировки сети. Каждый объект может перемещаться толь-

ко по позициям одной авторизации, номер которой определяется номером авторизации соответствующего транзакта. Перемещение объекта может осуществляться либо из входной позиции модуля в противолежащую ей выходную позицию того же модуля, либо из выходной позиции модуля во входную позицию той же авторизации другого модуля того же блока со спуском на один уровень ЭМЗАС, либо из выходной позиции модуля первого уровня во входную позицию той же авторизации модуля L-го уровня ЭМЗАС. Одновременно допустимо перемещение многих объектов (представление параллельных процессов). Для перемещения объекта из разрешающей позиции требуется предварительно вычислить соответствующую разрешающую процедуру для определения совокупности модулей, во входные позиции той же авторизации которых произойдет перемещение с возможным размножением или поглощением объектов. Длительность нахождения объекта в данной позиции определяется ее процедурой задержки. В конце этого интервала времени осуществляется перемещение с возможным размножением или поглощением объекта из одной позиции в другую, и над атрибутами перемещаемых объектов выполняется процедура преобразования.

ФОРМАЛЬНОЕ ЗАДАНИЕ СОСТАВА И СТРУКТУРЫ ЭМЗАС-СЕТИ

Введем следующие обозначения.

S — конечное непустое множество позиций, состоящее из непересекающихся подмножеств одинаковой мощности простых позиций Q и разрешающих позиций P: $S = Q \cup P$, $Q \cap P = \varnothing$, $|Q| = |P|$. Q — конечное непустое множество простых позиций, состоящее из непересекающихся подмножеств простых позиций различных уровней: $Q = \bigcup_{l=1}^{L} Q_l$, $Q_k \cap Q_l = \varnothing$, $k = \overline{1,L}$, $l = \overline{1,L}$, $k \neq l$. P — конечное непустое множество разрешающих позиций, состоящее из непересекающихся подмножеств разрешающих позиций различных уровней: $P = \bigcup_{l=1}^{L} P_l$, $P_k \cap P_l = \varnothing$, $k = \overline{1,L}$, $l = \overline{1,L}$, $k \neq l$. Для любого фиксированного уровня мощности множеств простых и разрешающих позиций данного уровня равны: $|Q_l| = |P_l|$, $l = \overline{1,L}$.

U — конечное непустое множество модулей, состоящее из непересекающихся подмножеств модулей различных уровней: $U = \bigcup_{l=1}^{13} U_l$, $U_k \cap U_l = \varnothing$, $k = \overline{1,L}$, $l = \overline{1,L}$, $k \neq l$; $|U_L| = 1$.

$I(u)$ — индекс модуля $u \in U$. Если $u \in U_L$, то $I(u) = 0$. Если $u \in U_{L-1}$, то $I(u) \in \overline{1,K[0]}$. Если $u \in U_{L-2}$, то $I(u) = i_1.i_2$, где $i_1 \in \overline{1,K[0]}$, $i_2 \in \overline{1,K[i_1]}$,.... Если $u \in U_1$, то $I(u) = i_1.i_2.i_3.....i_{L-1}$, где $i_1 \in \overline{1,K[0]}$, $i_2 \in \overline{1,K[i_1]}$, $i_3 \in \overline{1,K[i_1.i_2]}$,..., $i_{L-1} \in \overline{1,K[i_1.i_2.i_3.....i_{L-2}]}$.

Любой *модуль ЭМЗАС-сети заданной структуры* формально можно представить следующим кортежем:

$$u = \langle I, q = q[I,\alpha], p = p[I,\alpha] \rangle \in U, \qquad (1)$$

где $I = I(u)$ — индекс модуля, $\alpha = \overline{1,N}$ — номер авторизации, $q = q[I,\alpha]$ — простая позиция авторизации α данного модуля, $p = p[I,\alpha]$ — разрешающая позиция авторизации α данного модуля.

Структура самой ЭМЗАС-сети формально представляется кортежем

$$E = \langle N, K = K[I], r = r[I,\alpha], M_{\text{вх}} = M_{\text{вх}}[I,\alpha], M_{\text{вых}} = M_{\text{вых}}[I,\alpha] \rangle, \qquad (2)$$

где N — количество номеров авторизации, $K = K[I]$ — номер последнего модуля в блоке с индексом I, $r = r[I,\alpha]$ — признак допустимости авторизации α в модуле с индексом I, $M_{\text{вх}} = M_{\text{вх}}[I,\alpha]$ — входная функция разметки, определяющая маркировку, или состояние, входных позиций модулей в форме булевой переменной, $M_{\text{вых}} = M_{\text{вых}}[I,\alpha]$ — выходная функция разметки, определяющая маркировку, или состояние, выходных позиций модулей в форме булевой переменной. Функции разметки показывают, содержит ли данная позиция объект, причем каждая позиция может содержать не более одного объекта.

ФОРМАЛЬНОЕ ЗАДАНИЕ ПОЛИТИК БЕЗОПАСНОСТИ

Глобальная ПБ эталонной АС в смысле ЭМЗАС — это полномочия дискреционного

доступа заданной авторизации к защищаемой информации как объектам уровня физических ресурсов АС (полномочия данного пользователя в данной роли по использованию физической среды хранения и передачи информации с учетом размещения в ней конкретных элементов защищаемой информации). Ее математической моделью служит *глобальная ПБ на ЭМЗАС-сети*, задаваемая множеством *разрешенных ею позиций* как подмножеством разрешающих позиций первого уровня: $\Omega_{\text{г}} \subseteq 2^{P_1}$.

Выполнение заданной глобальной ПБ $\Omega_{\text{г}}$ *на ЭМЗАС-сети* означает:

$$(\forall p = p[I,\alpha] \in P_1 \setminus \Omega_{\text{г}})(M_{\text{вых}}[I,\alpha] = 0), \quad (3)$$

т.е. никакая разрешающая позиция первого уровня, не являющаяся разрешенной, не может содержать объект. Это интерпретируется как невозможность нелегального с точки зрения заданной глобальной ПБ эталонной АС дискреционного доступа. *Нарушение (актуальное или потенциальное) заданной глобальной ПБ* $\Omega_{\text{г}}$ *на ЭМЗАС-сети* характеризуется актуальной или потенциальной ситуацией:

$$(\exists p = p[I,\alpha] \in P_1 \setminus \Omega_{\text{г}})(M_{\text{вых}}[I,\alpha] = 1), \quad (4)$$

т.е. некоторая разрешающая, но не разрешенная позиция первого уровня содержит объект. Это интерпретируется как нелегальный для заданной глобальной ПБ эталонной АС дискреционный доступ пользователя к физическим ресурсам АС.

Обобщением глобальной ПБ эталонной АС на произвольный уровень ЭМЗАС является *уровневая дискреционная ПБ эталонной АС* — полномочия дискреционного доступа заданной авторизации к объектам данного уровня (полномочия данного пользователя в данной роли по использованию ресурсов данного уровня). Для математического моделирования определим *уровневую дискреционную ПБ на ЭМЗАС-сети*, задаваемую множеством *разрешенных ею позиций* как подмножеством разрешающих позиций данного (l-го) уровня: $\Omega_{\text{д}l} \subseteq 2^{P_l}$. В АС и на ЭМЗАС-сети дискреционная ПБ первого уровня есть глобальная ПБ.

Выполнение уровневой дискреционной ПБ $\Omega_{\text{д}l}$ *на ЭМЗАС-сети* означает:

$$(\forall p = p[I,\alpha] \in P_l \setminus \Omega_{\text{д}l})(M_{\text{вых}}[I,\alpha] = 0), \quad (5)$$

т.е. никакая разрешающая, но не разрешенная позиция данного (l-го) уровня не может содержать объект. Это интерпретируется как выполнение заданной уровневой дискреционной ПБ эталонной АС. *Нарушение (актуальное или потенциальное) ПБ* $\Omega_{\text{д}l}$ характеризуется актуальной или потенциальной ситуацией:

$$(\exists p = p[I,\alpha] \in P_l \setminus \Omega_{\text{д}l})(M_{\text{вых}}[I,\alpha] = 1), \quad (6)$$

т.е. некоторая разрешающая, но не разрешенная позиция данного (l-го) уровня содержит объект. Это интерпретируется как нелегальный для данной ПБ дискреционный доступ пользователя к объектам данного уровня.

Правила безопасного межсубъектного управления в эталонной АС декомпозируются по уровням ЭМЗАС в соответствии с аналогичной классификацией пар субъектов «управляющий — управляемый». Любой субъект может управлять субъектом только соседнего нижестоящего уровня. Уровневые правила оперируют субъектами данного уровня как управляемыми и соседнего вышестоящего уровня как управляющими. Такая ПБ (*уровневая локальная ПБ эталонной АС*), относясь к взаимодействию соседних уровней, носит локальный характер в отличие от дискреционной ПБ, связывающей уровни от верхнего до данного, и, тем более, от глобальной ПБ, охватывающей все уровни ЭМЗАС.

Для математического моделирования введем понятие *уровневой локальной ПБ на ЭМЗАС-сети*, задаваемой для данного (l-го) уровня как множество

$$\Omega_{\text{л}l} = \left\{ \left\langle I(u), \alpha, r[I(u),\alpha] \right\rangle \middle| u \in U_l, \alpha = \overline{1,N} \right\}. \quad (7)$$

Такая ПБ устанавливает признаки допустимости авторизаций в модулях данного уровня (допустимость перемещения объекта из простой позиции в разрешающую для каждой пары противолежащих позиций данного уровня). Множество *позиций, разрешенных уровневой локальной ПБ* $\Omega_{\text{л}l}$ *на ЭМЗАС-сети* (разрешающие позиции данного уровня, в которые допустимо перемещение объекта) имеет вид:

$$\left\{ p = p\left[I(u),\alpha\right] \in \right.$$
$$\left. \in P_l \middle| u \in U_l, \alpha = \overline{1,N}, \left\langle I(u), \alpha, 1 \right\rangle \in \Omega_{\text{л}l} \right\}.$$

Выполнение уровневой локальной ПБ $\Omega_{лl}$ *на ЭМЗАС-сети* означает:

$$(\forall p = p[I(u),\alpha] \in P_l \,|\, u \in U_l, \alpha = \overline{1,N}, \\ \langle I(u),\alpha,0\rangle \in \Omega_{лl})(M_{вых}[I,\alpha] = 0), \quad (8)$$

т.е. никакая разрешающая, но не разрешенная позиция данного (l-го) уровня не может содержать объект. Это интерпретируется как выполнение уровневой локальной ПБ эталонной АС. *Нарушение ПБ* $\Omega_{лl}$ означает:

$$(\exists p = p[I(u),\alpha] \in P_l \,|\, u \in U_l, \alpha = \overline{1,N}, \\ \langle I(u),\alpha,0\rangle \in \Omega_{лl})(M_{вых}[I,\alpha] = 1), \quad (9)$$

т.е. некоторая разрешающая, но не разрешенная позиция данного (l-го) уровня содержит объект (интерпретируется как нарушение уровневой локальной ПБ АС).

Правила безопасного межсубъектного управления в эталонной АС декомпозируются также по управляющим субъектам. Математической моделью межсубъектного управления с фиксированным управляющим субъектом является блок ЭМЗАС-сети. При этом для произвольного блока ЭМЗАС-сети с индексом I его единственный верхний модуль (№ 0 в блоке и с индексом I в ЭМЗАС-сети) ассоциируется с управляющим субъектом, а все его нижние модули (с номерами от 1 до $K[I]$ в блоке и с индексами от $I.1$ до $I.K[I]$ в ЭМЗАС-сети ассоциируются с актуально или потенциально управляемыми субъектами. Для математического моделирования правил безопасного межсубъектного управления с фиксированным управляющим субъектом введем понятие *блочной ПБ на ЭМЗАС-сети*, устанавливающей признаки допустимости всевозможных авторизаций во всех модулях данного блока (допустимость перемещения объекта из простой позиции в разрешающую для каждой пары противолежащих позиций данного блока).

При формальном задании такой ПБ возникает вопрос согласования признаков допустимости авторизаций и соответствующих множеств *разрешенных позиций* (разрешающие позиции данного блока, в которые допустимо перемещение объекта) между верхним модулем, с одной стороны, и всеми нижними модулями, с другой. Предпосылкой согласования является одинаковая авторизация управляемого и управляющего субъектов в эталонной АС. На ЭМЗАС-сети это проявляется в том, что объект попадает в разрешающую позицию нижнего модуля только из аналогично авторизованной разрешающей позиции верхнего модуля. Как следствие: во-первых, допустимость авторизации для управляемого субъекта требует допустимости той же авторизации для управляющего; во-вторых, недопустимость авторизации для управляющего субъекта требует недопустимости той же авторизации для всех управляемых. Первое и второе следствия дают соответственно ***первое (10) и второе (11) правила согласования признаков допустимости авторизации при формальном задании блочной ПБ на ЭМЗАС-сети*:**

$$(\exists j \in \overline{1,K[I]})(r[I.j,\alpha] = 1) \Rightarrow (r[I,\alpha] = 1), \\ \alpha = \overline{1,N},\ I = I(u),\ u \in U \setminus U_1; \quad (10)$$

$$(r[I,\alpha] = 0) \Rightarrow (\forall j \in \overline{1,K[I]})(r[I.j,\alpha] = 0), \\ \alpha = \overline{1,N},\ I = I(u),\ u \in U \setminus U_1. \quad (11)$$

Блочная ПБ на ЭМЗАС-сети задается согласованной по этим правилам установкой признаков допустимости авторизаций во всех модулях данного блока.

Для математического моделирования взаимно согласованных по всей эталонной АС правил безопасного межсубъектного управления определим понятие *локальной ПБ на ЭМЗАС-сети* как объединение уровневых локальных ПБ по всем уровням с согласованием признаков допустимости авторизации в рамках блочной ПБ по всем блокам. Задавать такую ПБ можно множеством

$$\Omega_{л} = \bigcup_{l=1}^{L} \Omega_{лl} = \\ = \left\{\langle I(u),\alpha,r[I(u),\alpha]\rangle \,|\, u \in U, \alpha = \overline{1,N}\right\}, \quad (12)$$

где все признаки $r[I(u),\alpha]$ взаимно согласованы по всем блокам.

Будем говорить, что индекс J является *подиндексом индекса* I, и обозначать это $J \subset I$ или $I \supset J$, если $I = J.i_1.i_2.\ldots.i_k$. Введение понятия подиндекса позволяет объединять по всем уровням отдельно первое и отдельно второе правила согласования при-

знаков допустимости авторизации, что дает соответственно ***первое (13) и второе (14) правила согласования признаков допустимости авторизации при формальном задании локальной ПБ на ЭМЗАС-сети:***

$$(r[I,\alpha]=1)\Rightarrow(\forall J\subset I)(r[J,\alpha]=1),\quad \alpha=\overline{1,N},\ I=I(u),\ u\in U\setminus U_L. \tag{13}$$

$$(r[I,\alpha]=0)\Rightarrow(\forall J\supset I)(r[J,\alpha]=0),\quad \alpha=\overline{1,N},\ I=I(u),\ u\in U\setminus U_1. \tag{14}$$

Для математического моделирования согласованных по всей АС полномочий дискреционного доступа определим понятие *дискреционной ПБ на ЭМЗАС-сети* как объединение уровневых дискреционных ПБ по всем уровням с их согласованием в рамках каждой блочной ПБ. Задавать такую ПБ можно множеством

$$\Omega_{др}=\bigcup_{l=1}^{L}\Omega_{дl}\subseteq 2^P, \tag{15}$$

где множества $\Omega_{дl}$ согласованы по блокам. Согласование разрешенных позиций и признаков допустимости авторизации эквивалентно (разрешенная позиция — истинное значение признака, а неразрешенная — ложное). Эквивалентно (10) и (11) получаем соответственно ***первое (16) и второе (17) правило согласования разрешенных позиций при формальном задании блочной ПБ на ЭМЗАС-сети:***

$$(\exists j\in\overline{1,K[I]})(p[I.j,\alpha]\in\Omega_{др})\Rightarrow(p[I,\alpha]\in\Omega_{др}),\quad \alpha=\overline{1,N},\ I=I(u),\ u\in U\setminus U_1, \tag{16}$$

$$(p[I,\alpha]\notin\Omega_{др})\Rightarrow(\forall j\in\overline{1,K[I]})(p[I.j,\alpha]\notin\Omega_{др}),\quad \alpha=\overline{1,N},\ I=I(u),\ u\in U\setminus U_1. \tag{17}$$

Объединение по всем уровням правил (16) и (17) дает соответственно ***первое (18) и второе (19) правило согласования разрешенных позиций при формальном задании дискреционной ПБ на ЭМЗАС-сети:***

$$(p[I,\alpha]\in\Omega_{др})\Rightarrow(\forall J\subset I)(p[J,\alpha]\in\Omega_{др}),\quad \alpha=\overline{1,N},\ I=I(u),\ u\in U\setminus U_L. \tag{18}$$

$$(p[I,\alpha]\notin\Omega_{др})\Rightarrow(\forall J\supset I)(p[J,\alpha]\notin\Omega_{др}),\quad \alpha=\overline{1,N},\ I=I(u),\ u\in U\setminus U_1. \tag{19}$$

Дискреционную ПБ на ЭМЗАС-сети можно задавать согласованным по этим правилам множеством разрешенных позиций (*разрешающее* представление).

Разрешающее представление дискреционной ПБ на ЭМЗАС-сети информационно избыточно вследствие (18)—(19), т.е. дискреционную ПБ можно однозначно задавать не только множеством всех разрешенных данной ПБ позиций, но и некоторым его подмножеством, по которому можно однозначно восстановить все множество. Для устранения информационной избыточности введем *глобализованное представление дискреционной ПБ на ЭМЗАС-сети*, задаваемое посредством *глобализованного множества* $\Omega_{дг}$ *разрешенных позиций*, которое выразим через разрешающее представление $\Omega_{др}$ следующим образом:

$$(p[I,\alpha]\in\Omega_{дг})\Leftrightarrow\Leftrightarrow((p[I,\alpha]\in\Omega_{др})\wedge(\forall J\supset I)(p[J,\alpha]\notin\Omega_{др})),\quad \alpha=\overline{1,N},\ I=I(u),\ u\in U. \tag{20}$$

Из этого определения следует, в частности, что $\Omega_{дг}\subseteq\Omega_{др}$.

Теорема 1. *Разрешающее представление* $\Omega'_{др}$ *дискреционной ПБ на ЭМЗАС-сети можно выразить через ее глобализованное представление* $\Omega_{дг}$ *так:*

$$(p[I,\alpha]\in\Omega'_{др})\Leftrightarrow\Leftrightarrow((p[I,\alpha]\in\Omega_{дг})\vee(\exists J\supset I)(p[J,\alpha]\in\Omega_{дг})),\quad \alpha=\overline{1,N},\ I=I(u),\ u\in U. \tag{21}$$

Теорема 2. *Пусть на ЭМЗАС-сети задана дискреционная ПБ с глобализованным представлением* $\Omega_{дг}$. *Тогда имеет место формула:*

$$(p'=p[I',\alpha]\in\Omega_{дг}\wedge p''=p[I'',\alpha]\in\Omega_{дг})\Rightarrow\Rightarrow(I'\not\subset I''\wedge I''\not\subset I'), \tag{22}$$

то есть для любых двух позиций одинаковой авторизации из глобализованного множества разрешенных позиций индекс одной из этих позиций не может быть подиндексом другой.

Теорема 3. *Всякое подмножество* $\Omega_{дг}\subset P$ *множества разрешающих позиций* P *ЭМЗАС-сети, удовлетворяющее (22), однозначно задает на ней глобализованное*

представление некоторой дискреционной ПБ.

Теорема 4 (существования и единственности глобализованного представления дискреционной ПБ на ЭМЗАС-сети). *Любая дискреционная ПБ на ЭМЗАС-сети имеет свое единственное глобализованное представление.*

Взаимно однозначное соответствие между дискреционными ПБ на ЭМЗАС-сети и подмножествами множества разрешающих позиций, удовлетворяющими (22), устанавливается глобализованным представлением $\Omega_{дг}$. Задавая его, можно построить разрешающее представление $\Omega_{др}$ этой же ПБ согласно (21). Для этого нужно для каждой позиции из $\Omega_{дг}$ включить в $\Omega_{др}$ ее саму и все позиции той же авторизации, индекс которых является подиндексом данной. *Выполнение дискреционной ПБ на ЭМЗАС-сети* с разрешающим представлением $\Omega_{др}$ означает:

$$(\forall p = p[I,\alpha] \in P \setminus \Omega_{др})(M_{вых}[I,\alpha] = 0), \quad (23)$$

т.е. никакая разрешающая, но не разрешенная данной ПБ позиция не может содержать объект. Это интерпретируется как невозможность нелегального для заданной дискреционной ПБ АС дискреционного доступа. *Нарушение (актуальное или потенциальное) дискреционной ПБ на ЭМЗАС-сети* с разрешающим представлением $\Omega_{др}$ характеризуется актуальной или потенциальной ситуацией:

$$(\exists p = p[I,\alpha] \in P \setminus \Omega_{др})(M_{вых}[I,\alpha] = 1), \quad (24)$$

т.е. некоторая разрешающая, но не разрешенная позиция содержит объект. Это интерпретируется как нелегальный для заданной дискреционной ПБ АС доступ.

ИНДУЦИРОВАНИЕ ПОЛИТИК БЕЗОПАСНОСТИ НА ЭМЗАС-СЕТИ

В эталонной АС гарантирование заданной дискреционной ПБ достигается поддержанием соответствующей локальной ПБ. В этом смысле можно говорить об *индуцировании соответствующей локальной политикой безопасности гарантируемой дискреционной политики безопасности в эталонной АС*. Математической моделью этого является аналогичное индуцирование на ЭМЗАС-сети.

Будем говорить, что *локальная ПБ* $\Omega_{л}$ *на ЭМЗАС-сети, определенная через (12), индуцирует дискреционную ПБ на ЭМЗАС-сети с разрешающим представлением* $\Omega_{др}$, *определенным через (15)*, если выполнено:

$$(\forall p = p[I,\alpha] \in P)((p \in \Omega_{др}) \Leftrightarrow (r[I,\alpha] = 1)). \quad (25)$$

Так как согласование признаков допустимости авторизации эквивалентно согласованию разрешенных позиций, существует взаимно однозначное соответствие между индуцирующими локальными ПБ и индуцируемыми дискреционными ПБ.

Теорема 5 (основная теорема безопасности для дискреционной ПБ на ЭМЗАС-сети). *Если в начальный момент времени выполняется заданная дискреционная ПБ на ЭМЗАС-сети, и все перемещения объектов удовлетворяют индуцирующей ее локальной ПБ, то в любой последующий момент времени эта заданная дискреционная ПБ также выполняется.*

Будем говорить, что *некоторая (конечная) маркировка ЭМЗАС-сети достижима из некоторой другой (начальной) маркировки в рамках заданной локальной ПБ*, если конечную маркировку можно получить из начальной в результате некоторой последовательности перемещения объектов, причем при каждом таком перемещении объекта будет выполняться заданная ПБ.

Будем называть следующую *маркировку ЭМЗАС-сети корневой*:

$$\begin{aligned}(\forall p = p[I,\alpha] \in P_L)(M_{вх}[I,\alpha] = \\ = 1 \wedge M_{вых}[I,\alpha] = 0) \wedge \\ \wedge(\forall p = p[I,\alpha] \in P \setminus P_L)(M_{вх}[I,\alpha] = \\ = M_{вых}[I,\alpha] = 0),\end{aligned} \quad (26)$$

то есть все простые позиции верхнего уровня содержат объект, но никакая из остальных позиций ЭМЗАС-сети не содержит объект. Корневая маркировка ЭМЗАС-сети интерпретируется как отсутствие гиперпроцессов в эталонной АС.

Будем называть следующую *маркировку ЭМЗАС-сети индуцированной дискреционной ПБ с заданным глобализованным представлением* $\Omega_{дг}$:

$$(\forall p = p[I,\alpha] \in \Omega_{\text{дг}})(M_{\text{вх}}[I,\alpha] = 0 \wedge M_{\text{вых}}[I,\alpha] = 1) \wedge$$
$$\wedge(\forall p = p[I,\alpha] \in P \setminus \Omega_{\text{дг}})(M_{\text{вх}}[I,\alpha] = M_{\text{вых}}[I,\alpha] = 0), \quad (27)$$

то есть все позиции из глобализованного множества разрешенных данной дискреционной ПБ позиций содержат объект, но никакая из остальных позиций ЭМЗАС-сети не содержит объект. Такую маркировку ЭМЗАС-сети можно интерпретировать как реализацию дискреционного доступа к ресурсам эталонной АС с полномочиями, максимально предусмотренными заданной дискреционной ПБ.

Теорема 6 (основная теорема достижимости для дискреционной ПБ на ЭМЗАС-сети). *Для любой заданной дискреционной ПБ всегда можно так определить разрешающие процедуры и процедуры преобразования на ЭМЗАС-сети, что индуцированная данной дискреционной ПБ маркировка ЭМЗАС-сети окажется достижимой из корневой маркировки в рамках индуцирующей данную дискреционную ПБ локальной ПБ.*

Основные теоремы безопасности и достижимости для дискреционной ПБ на ЭМЗАС-сети имеют естественную интерпретацию: для любой заданной дискреционной ПБ эталонной АС однозначно определяются поддерживающие ее правила безопасного межсубъектного управления, при выполнении которых возможен легальный дискреционный доступ и невозможен нелегальный.

Для математического моделирования механизмов поддержания заданных полномочий дискреционного доступа к объектам на уровне физических ресурсов АС, введем понятия индуцирования глобальной политики безопасности дискреционной и локальной политиками безопасности на ЭМЗАС-сети.

Будем говорить, что *дискреционная ПБ с глобализованным представлением* $\Omega_{\text{дг}}$ *индуцирует глобальную ПБ на ЭМЗАС-сети* $\Omega_{\text{г}}$, если $\Omega_{\text{г}} = \Omega_{\text{дг}}$.

В силу теоремы 3 всякое подмножество $\Omega_{\text{дг}} \subset P$ множества разрешающих позиций, удовлетворяющее (22), однозначно задает глобализованное представление некоторой дискреционной ПБ. Подмножество $\Omega_{\text{г}} \subset P$ удовлетворяет (22), так как все его позиции относятся к одному (первому) уровню. Поэтому любая глобальная ПБ индуцируется единственной дискреционной ПБ на ЭМЗАС-сети. А она, в свою очередь, индуцируется некоторой локальной ПБ.

Будем говорить, что *заданная локальная ПБ на ЭМЗАС-сети индуцирует заданную глобальную ПБ на ЭМЗАС-сети*, если индуцирующая заданную глобальную ПБ дискреционная ПБ индуцируется заданной локальной ПБ.

Так как любая глобальная ПБ индуцируется единственной дискреционной ПБ, а любая дискреционная ПБ индуцируется единственной локальной ПБ, то любая глобальная ПБ индуцируется единственной локальной ПБ. Легко видеть, что выполнение индуцирующей заданную глобальную ПБ дискреционной ПБ означает одновременно и выполнение заданной глобальной ПБ.

Теорема 7 (основная теорема безопасности для глобальной ПБ на ЭМЗАС-сети). *Если в начальный момент времени выполняется индуцирующая заданную глобальную ПБ дискреционная ПБ на ЭМЗАС-сети, и все перемещения объектов удовлетворяют индуцирующей заданную глобальную ПБ локальной ПБ, то в любой последующий момент будет выполняться заданная глобальная ПБ.*

Будем называть *маркировку ЭМЗАС-сети индуцированной заданной глобальной ПБ*, если данная маркировка индуцирована дискреционной ПБ, индуцирующей заданную глобальную ПБ. Для любой глобальной ПБ индуцированная ею маркировка определяется однозначно: все позиции из множества разрешенных позиций содержат объект, но никакая из остальных позиций ЭМЗАС-сети не содержит. Это можно интерпретировать как реализацию дискреционного доступа ко всей информации, на которую имеются полномочия доступа.

Теорема 8 (основная теорема достижимости для глобальной ПБ на ЭМЗАС-сети). *Для любой заданной глобальной ПБ всегда можно так определить разрешающие процедуры и процедуры преобразования на ЭМЗАС-сети, что индуцированная данной глобальной ПБ маркировка ЭМЗАС-сети окажется достижимой из корневой в рамках индуцирующей данную глобальную ПБ локальной ПБ.*

Основные теоремы безопасности и достижимости для глобальной ПБ на ЭМЗАС-сети имеют естественную интерпретацию: для любой заданной глобальной ПБ эталонной АС однозначно определяются поддерживающие ее правила безопасного межсубъектного управления, при выполнении которых возможен легальный в рамках такой глобальной ПБ доступ и невозможен нелегальный.

ЗАКЛЮЧЕНИЕ

Построена математическая модель ПБ эталонной АС в смысле ЭМЗАС, для чего определены различные ПБ на ЭМЗАС-сети: глобальная, уровневая дискреционная, уровневая локальная, блочная, локальная и дискреционная. Определены способы их формального задания, для дискреционной ПБ предложены два представления: разрешающее и глобализованное. Математическая модель ПБ эталонной АС гарантирует «хорошие» свойства частных ПБ на ЭМЗАС-сети и позволяет получать эффективные утверждения (для всех них разработаны доказательства, которые не удалось здесь привести ввиду ограниченности объема статьи). Прежде всего, это основные теоремы безопасности и достижимости. Такие утверждения характеризуют математические свойства ЭМЗАС-сети как модели безопасной технологии циркуляции информации в АС, служащие инструментом разработки АС КП. Тем самым, построенная математическая модель ПБ эталонной АС дает математическое основание для формулирования, изучения и реализации ПБ эталонной АС, что создает существенные теоретические предпосылки для реализации концепции эталонной АС в смысле ЭМЗАС в практике разработки АС КП.

СПИСОК ЛИТЕРАТУРЫ

1. *Дубровин А.С.* Требования к субъектному наполнению эталонной автоматизированной системы при организации изолированной программной среды // Всерос. науч.-практ. конф. «Современные проблемы борьбы с преступностью»: Сб. матер. (радиотехн. науки). — Воронеж: ВИ МВД России, 2004. — С. 54—55.

2. *Костин А.Е., Шаньгин В.Ф.* Организация и обработка структур данных в вычислительных системах: Учеб. пособ. для вузов. — М.: Высш. шк., 1987. — 248 с.

3. *Дубровин А.С.* ЭМЗАС-сети как аппарат моделирования безопасных технологий циркуляции информации в автоматизированных системах / А. С. Дубровин, В. И. Сумин // Матер. XLIII отчетной науч. конф. за 2004 г. — Воронеж: Воронеж. гос. технол. акад., 2005. — Ч. 3. — С. 91.

4. *Дубровин А.С.* Политика бесконфликтного межсубъектного взаимодействия в эталонной модели защищенной автоматизированной системы / А .С. Дубровин, В. И. Сумин // Теория конфликта и ее приложения: Матер. III Всерос. науч.-техн. конф. — Воронеж: Научная книга, 2004. — С. 331—334.

5. *Щербаков А.Ю.* Введение в теорию и практику компьютерной безопасности. — М.: издатель Молгачева С.В., 2001. — 352 с.