УДК 681.3

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОДСИСТЕМЫ ЭТАЛОННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОБРАБОТКИ ДАННЫХ НА ОСНОВЕ ЭМЗАС-СЕТИ

А.С. Дубровин [1]
В.И. Сумин [2]

[1] *Воронежская государственная технологическая академия*

[2] *Воронежский институт МВД России*

e-mail: asd_kiziltash@box.vsi.ru

Построены на основе аппарата ЭМЗАС-сетей математические модели регламентируемой эталонной моделью защищенной автоматизированной системы (ЭМЗАС) политики безопасности (ПБ) отдельной подсистемы автоматизированной системы обработки данных (АСОД). Построенные модели дают основу для синтеза ПБ эталонной АСОД по подсистемам, что существенно расширяет теоретические предпосылки для реализации ЭМЗАС в практике разработки АСОД критического применения.

Ключевые слова: эталонная модель защищенной автоматизированной системы (ЭМЗАС), автоматизированная система обработки данных (АСОД) критического применения (КП), дискреционный доступ, основная теорема безопасности, суперблок ЭМЗАС-сети.

Данная работа посвящена обобщению математических моделей, опубликованных в [1], с учетом некоторых структурных аспектов, начало исследованию которых положила статья [2]. Предварительно кратко изложим современное состояние вопроса.

Современный взгляд на понятие защищенности от несанкционированного доступа (НСД) автоматизированной информационной системы (АИС) поддерживается на международном уровне стандартом ISO/IEC 15408, кратко называемым также ОК – «Общие критерии», и на отечественном уровне группой стандартов ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Согласно этому взгляду, защищенная АИС – это АИС, которая успешно противодействует заданным угрозам защищенности при заданных внешних условиях ее функционирования. Защита информации (ЗИ) от НСД превращается в бесконечную гонку средств защиты и нападения, когда появление новых средств нападения приводит к появлению противостоящих им средств защиты, а появление новых средств защиты приводит к появлению обходящих их средств нападения.

Являясь удовлетворительным для многих классов АИС, такое понимание плохо подходит для класса автоматизированных систем обработки данных (АСОД) критического применения (КП). АСОД КП появились в результате внедрения вычислительной техники в сфере критических объектов (военные объекты, экологически опасные производства, атомные станции, объекты транспорта, связи, финансово-кредитной сферы и т.д.), характеризующихся неприемлемостью для общества ущерба от нарушения их работоспособности [3]. Требования к программно-технической реализации АСОД КП отличаются приоритетом защищенности от НСД над функциональностью. Для АСОД КП предпочтительнее перспективный взгляд, трактующий защищенность от НСД как отсутствие в технологии циркуляции информации уязвимостей, по причине наличия которых возможна реализация различных угроз, что позволит разорвать порочный круг бесконечного противостояния средств защиты и нападения.

Защищенность АСОД КП должна характеризоваться соответствием реализованной в ней технологии циркуляции информации некоторым подлежащим стандартизации эталонным моделям безопасной (неуязвимой) циркуляции информации. Однако в настоящее время перспективный взгляд на понятие защищенности от НСД в АСОД КП лишь частично реализуется на практике, так как не находит прямого отражения в соответствующих стандартах на унифицированные архитектурные решения,

удовлетворяющие общепринятым эталонным моделям безопасной циркуляции информации в АСОД КП. В качестве претендента на такую эталонную модель Дубровиным А.С. при поддержке ряда коллег развивается эталонная модель защищенной автоматизированной системы (ЭМЗАС)) как теоретическая основа унификации архитектурного облика АСОД КП за счет стандартизации интерфейсов сопряжения прикладных процессов с уровневыми комплексами сервисов безопасности на основе их декомпозиции по уровням доступа к ресурсам АСОД (ЭМЗАС предусматривает 15-уровневую структуризацию как расширение 7-уровневой структуризации OSI в направлении декомпозиции ее прикладного уровня) [4, 5].

Причиной сложности создания такого рода эталонных моделей являются принципиальные теоретические трудности моделирования процессов ЗИ от НСД, возникающие при попытке соединить перспективное понимание защищенности с гибкостью защитных механизмов. Природа этих трудностей достаточно сложна, но в самом общем виде может быть описана следующим образом: существующие математические формализмы защищенности информации, описанные, в частности, в [6], предполагают при моделировании неуязвимости динамическое, локальное и дискретное рассмотрение, а при моделировании гибкости защитных механизмов – статическое, глобальное и непрерывное. В ЭМЗАС преодоление трудностей моделирования осуществляется на пути интеграции передовых математических формализмов защищенности информации, конструктивно соединяющей противоположные рассмотрения. Обеспечить на уровне моделей недопущение уязвимостей и гибкость защитных механизмов представляется невозможным в рамках традиционной «аналитической» общенаучной парадигмы. Предлагаемый в ЭМЗАС системный подход предусматривает соединение неуязвимости и гибкости по каждому из трех аспектов защищенности (конфиденциальность, доступность и целостность) на пути подлинной интеграции процессов обработки и защиты данных.

В плане конфиденциальности и доступности информации гибкость защитных механизмов означает гибкость разграничения доступа к информации, а уязвимости кроются в модели используемой политики безопасности (ПБ) АСОД КП и в ее практической реализации [7]. Единственной подлинно гибкой является дискреционная модель ПБ, которая принципиально небезопасна, то есть неизбежно порождает уязвимости. С другой стороны, принципиально безопасен только класс моделей конечных состояний, берущий свое начало от мандатного метода контроля доступа. Однако возможности применения существующих моделей конечных состояний весьма ограничены ввиду их принципиальной негибкости. Этот недостаток данного класса моделей можно устранить, сблизив данный класс моделей с дискреционной моделью. Но этому мешает естественное для «аналитической» общенаучной парадигмы традиционно независимое рассмотрение процессов защиты данных от процессов обработки данных в АСОД, а отход от этого принципа требует масштабных и глубоких научных исследований.

Любая модель ПБ АСОД обязательно поддерживает глобальную ПБ, характеризующую желаемые свойства АСОД (синтаксис доступа), и может поддерживать локальную ПБ, характеризующую правила перехода АСОД между соседними состояниями (семантика доступа). Наличие поддержки локальной ПБ означает динамичность соответствующей модели, а отсутствие – статичность. Динамическая модель ПБ, в отличие от статической, накладывает ограничения на состояния АСОД. Если множество возможных состояний удается представить как вполне определенное конечное множество, то модель ПБ относится к классу моделей конечных состояний. Теоретическим основанием принципиальной безопасности моделей конечных состояний ПБ АСОД служит так называемая основная теорема безопасности, которая формулируется и доказывается отдельно для каждой модели [7]. В соответствии с ней, если в начальный момент времени глобальная ПБ выполняется и все переходы АСОД из состояния в состояние удовлетворяют соответствующей локальной ПБ, то в любой последующий момент времени глобальная ПБ также будет выполняться. Таким образом, уязвимости

в АСОД данного типа не заложены непосредственно в модель ПБ, а могут появиться только при практической реализации.

Дискреционная модель, устанавливающая полномочия доступа пользователей, в общем случае выступающих в определенных ролях, к объектам, вообще не оперируя переходами между состояниями АСОД, наиболее совершенным образом поддерживает глобальную ПБ. Однако, не относясь к моделям конечных состояний, она принципиально не безопасна. Актуальна разработка в рамках ЭМЗАС моделей комплексов ПБ, являющихся моделями конечных состояний по существу и дискреционными по форме. Единство существа и формы при этом означает, что любой дискреционный доступ может реализовываться только однозначно определяемой последовательностью переходов между конечными состояниями, для которой можно гарантировать ее безопасность. Для этого необходимо обеспечить необходимое разделение процессов, реализующих различные дискреционные доступы, для устранения взаимовлияния и обеспечить контролируемую однозначную реализацию каждого отдельно взятого дискреционного доступа. Произвольный дискреционный доступ представляется многоуровневым, осуществляющимся к иерархически структурированным ресурсам с последовательным спуском по иерархическим уровням цепочкой авторизованных доступов компонентов вышестоящего уровня к ресурсам компонентов соседнего нижестоящего уровня. Ограничения глобальной ПБ задаются согласно обычной дискреционной модели, а локальной – через задание полномочий доступа данной авторизации между субъектами соседних уровней в направлении сверху вниз. Выполнение гарантирующей глобальную ПБ локальной ПБ обеспечивается автоматически с использованием механизма задания требований к субъектному наполнению эталонной АСОД при организации изолированной программной среды (ИПС). Тем самым, ЭМЗАС развивает концепцию ИПС [7], лежащую в основе методологии гарантирования защиты АСОД и являющуюся расширением зарубежных подходов к реализации ядра безопасности в направлении учета контроля порождения субъектов.

Формализм ЭМЗАС должен интегрировать дискреционный формализм [6, 7], имеющий статический характер, и удобный для описания процессов обработки данных сетевой формализм [8], имеющий динамический характер. Он должен единым образом описывать динамический и статический доступ к информации, структурируемой методом, обеспечивающим единство рассмотрения глобальной и локальной ПБ. Для этого на базе известных Е-сетевых формализмов [8], возникших в развитие сетей Петри, в рамках ЭМЗАС предложен новый проблемно-ориентированный аппарат математического моделирования – ЭМЗАС-сети, эквивалентные Е-сетям специального вида. Введение ЭМЗАС-сетей открывает путь для систематического исследования их математических свойств как инструмента разработки АСОД КП на основе ЭМЗАС. На этом пути построены на основе аппарата ЭМЗАС-сетей математические модели ПБ эталонной АСОД (определены ПБ на всей ЭМЗАС-сети целиком) [1].

Затем была выявлена возможность анализа и синтеза ЭМЗАС-сети по частям [2], поэтому актуально обобщение данных моделей в направлении возможного задания ПБ не на всей ЭМЗАС-сети, а на произвольном представителе некоторого подходящего класса ее связных частей, одним из которых является ЭМЗАС-сеть целиком. Помимо прежних вопросов формального задания и индуцирования ПБ, при этом возникают и имеющие существенное значение для развития методов синтеза ПБ совершенно новые вопросы совместимости ПБ, заданных на разных частях одной и той же ЭМЗАС-сети.

Исходной основой для удобного разбиения ЭМЗАС-сети на части служит вводимое для группирования нескольких соседних уровней ЭМЗАС по некоторому признаку понятие *слоя ЭМЗАС порядка j уровня* $l_в$ как совокупности уровней ЭМЗАС с номерами $l=\overline{l_н,l_в}$, где $l_н=l_в-j+1$ – номер *нижнего уровня данного слоя ЭМЗАС* [2]. Порядок и уровень слоя имеют смысл количества образующих уровней и наивысшего из них. Слой первого порядка уровня $l_в$ есть уровень с номером $l_в$.

Подходящим для математического моделирования ПБ эталонной АСОД специфическим синтаксическим представлением ЭМЗАС-сети является ее *каноническая форма* (см. рис. 1), найденная на основе минимизации описательных средств – граф особого вида, вершинами которого являются модули (см. рис. 2), содержащие позиции. Структура сети блочная (см. рис. 3), динамика определяется перемещением по заданным процедурам (преобразования, разрешающим и временной задержки) объектов (фишек), группирующихся в транзакты. Каждый *модуль ЭМЗАС-сети* 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.

Для идентификации модулей и блоков ЭМЗАС-сети используется механизм их индексации индексами различного порядка. Индекс произвольного j-го порядка определяется как выражение следующего вида: $i_1.i_2.\ \ldots\ .i_j$, 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 $(L-l)$, $l=\overline{1,L}$, 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 $I.j$. Будем говорить, что индекс J является *подиндексом индекса I*, и обозначать это $J\subset I$ или $I\supset J$, если $I=J.i_1.i_2.\ \ldots\ .i_k$. А ситуацию $((J\subset I)\vee(J=I))$ будем обозначать $J\subseteq I$ или $I\supseteq J$.

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 АСОД быть инициирован из соответствующего модуля процесс с данной авторизацией.

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 фишек. Динамика ЭМЗАС-сети в канонической форме определяется перемещением фишек из одних позиций в другие, что формально эквивалентно изменению маркировки сети. Каждая фишка может перемещаться только по позициям одной авторизации, номер которой определяется номером авторизации соответствующего транзакта.

Перемещение фишки может осуществляться либо из входной позиции модуля в противолежащую ей выходную, 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 фишек (представление параллельных процессов). Для перемещения фишки 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 фишек. Длительность нахождения фишки в данной позиции опре-

деляется ее процедурой задержки. В конце этого интервала времени осуществляется перемещение с возможным размножением или поглощением фишки из одной позиции в другую, и над атрибутами перемещаемых фишек выполняется процедура преобразования.

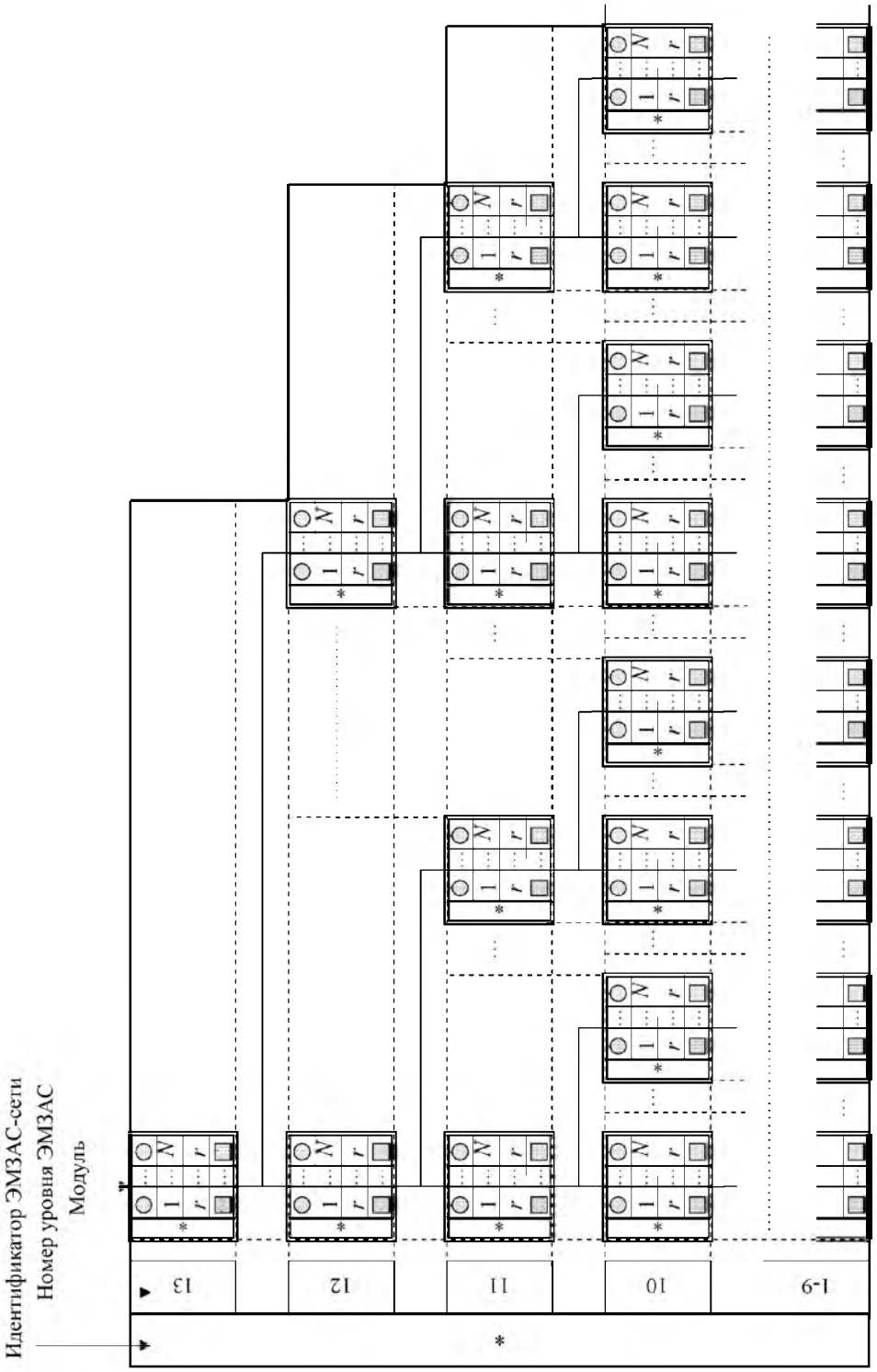

Рис. 1. Графическое изображение ЭМЗАС-сети в канонической форме

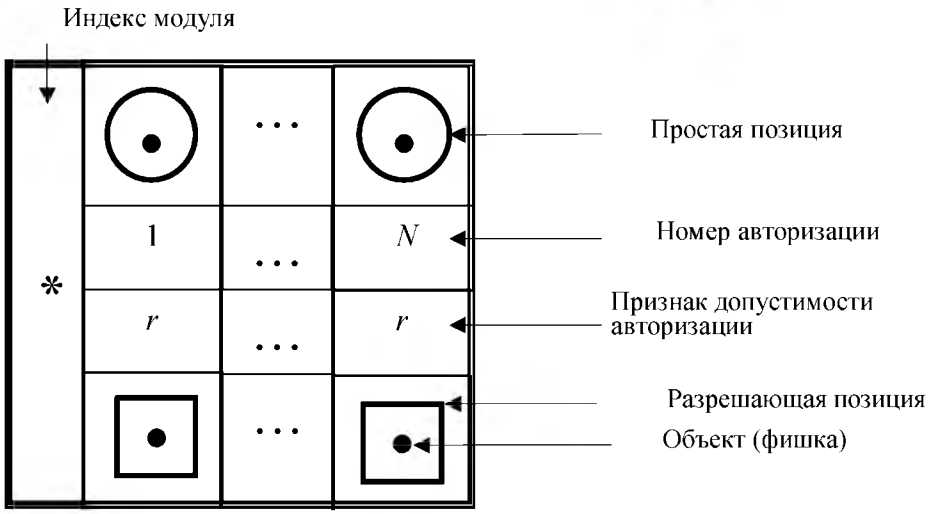

Рис. 2. Графическое изображение модуля ЭМЗАС-сети

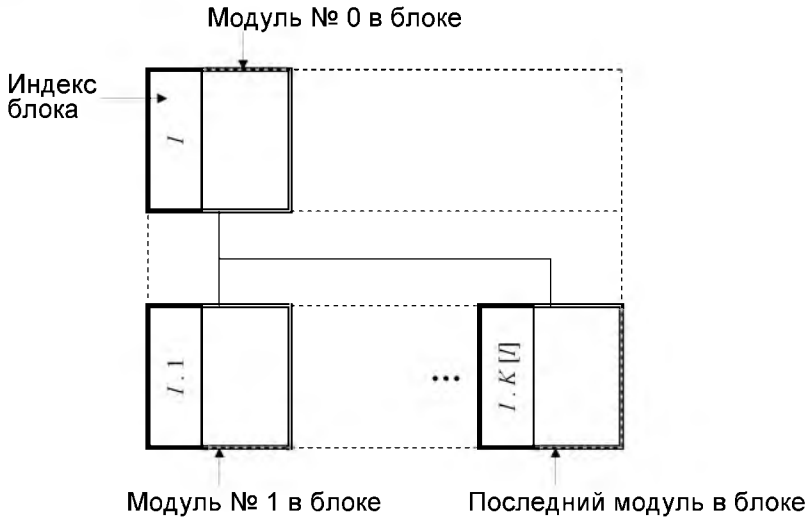

Рис. 3. Графическое изображение блока ЭМЗАС-сети

Введем следующие обозначения (везде $k=\overline{1,L}$, $l=\overline{1,L}$, $k\neq l$):

S – множество позиций, $S=Q\cup P\neq\varnothing$, $Q\cap P=\varnothing$, $|S|<\infty$, $|Q|=|P|$;

Q – множество простых позиций, $Q=\bigcup\limits_{l=1}^{L}Q_l\neq\varnothing$, $|Q|<\infty$, $Q_k\cap Q_l=\varnothing$;

P – множество разрешающих позиций, $P=\bigcup\limits_{l=1}^{L}P_l\neq\varnothing$, $|P|<\infty$, $P_k\cap P_l=\varnothing$;

Q_l, P_l – множества простых и разрешающих позиций l-го уровня, $|Q_l|=|P_l|\neq 0$;

U – множество модулей, $U=\bigcup\limits_{l=1}^{L}U_l\neq\varnothing$, $|U|<\infty$, $U_k\cap U_l=\varnothing$;

U_l – множество модулей l-го уровня;

$I(u)=i_1.i_2.i_3.\ldots.i_{L-1}$ – индекс модуля $u\in U_l$ и блока, у которого этот модуль верхний (№ 0 в блоке), в частности, $I(u)=0$ при $l=L$;

$K[I]$ – число нижних модулей в блоке с индексом I;

$I.j$ – индекс нижнего модуля с номером $j=\overline{1,K[I]}$ в блоке с индексом I;

$r=r[I,\alpha]$ – признак допустимости авторизации α в модуле с индексом I;

$M_{вх}=M_{вх}[I,\alpha]$, $M_{вых}=M_{вых}[I,\alpha]$ – входная и выходная функции разметки, определяющие маркировку, или состояние, входных и выходных позиций модулей в форме булевой переменной (показывают, маркирована ли данная позиция, т.е. содержит ли фишку, причем каждая позиция может содержать не более одной фишки).

Формальное представление *модуля ЭМЗАС-сети заданной структуры*:

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

где $I=I(u)$ – индекс модуля, $q=q[I,\alpha]\in Q_l$, $p=p[I,\alpha]\in P_l$.

Структура самой ЭМЗАС-сети формально представляется кортежем

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

Для проработки вопросов, связанных с совместным функционированием процессов эталонной АСОД в пределах некоторой ее подсистемы, вводятся в рассмотрение необходимые понятия в *сетевой* и более общей, *системной трактовке* для некоторых структурных компонент ЭМЗАС-сети. В сетевой трактовке структурный компонент ЭМЗАС-сети есть некоторая связная ее часть, а в системной – некоторое подмножество фиксированного множества U модулей ЭМЗАС-сети. Любой структурный компонент в сетевой трактовке отождествляется с соответствующим компонентом в системной, но компоненты в системной трактовке могут не иметь аналогов в сетевой. Определенные классы структурных компонент ЭМЗАС-сети трактуются в системной трактовке как системы множеств. Это позволяет применять к структурным компонентам любые теоретико-множественные операции, в частности: объединение, пересечение, вычитание, образование симметрической разности. Операции в такой трактовке полностью соответствуют операциям в сетевой трактовке, но имеют более общий характер, так как позволяют снять соответствующие ограничения замкнутости.

Слой $S_{l_н\ldots l_в}$ *уровня* $l_в$ *с нижним уровнем* $l_н$ *ЭМЗАС-сети* $B_0=S_{1\ldots L}$ (имеет *порядок* $j=l_в-l_н+1$) – это (в сетевой трактовке) часть ЭМЗАС-сети, относящаяся к слою ЭМЗАС порядка j уровня $l_в$. Он содержит только модули, относящиеся к данному слою ЭМЗАС, и связывающие их дуги. Для слоя первого порядка имеем: $S_{l_в\ldots l_в}=U_{l_в}$.

Два слоя ЭМЗАС-сети $S_{l_{н1}\ldots l_{в1}}$ *и* $S_{l_{н2}\ldots l_{в2}}$ будем называть *пересекающимися*, если они имеют хотя бы один общий образующий их уровень ЭМЗАС ($\max(l_{н1},l_{н2})\le\min(l_{в1},l_{в2})$), и *непересекающимися* в противном случае.

Для пары пересекающихся слоев ЭМЗАС-сети можно определить в сетевой трактовке операции объединения и пересечения следующим образом.

Результат *объединения двух пересекающихся слоев* $S_{l_{н1}\ldots l_{в1}}$ и $S_{l_{н2}\ldots l_{в2}}$ ЭМЗАС-сети есть слой $S_{l_н\ldots l_в}=S_{l_{н1}\ldots l_{в1}}\cup S_{l_{н2}\ldots l_{в2}}$, где $l_н=\min(l_{н1},l_{н2})$, $l_в=\max(l_{в1},l_{в2})$, этой ЭМЗАС-сети, образованный такими и только такими уровнями ЭМЗАС, которые образуют хотя бы один из исходных слоев.

Результат *пересечения двух пересекающихся слоев* $S_{l_{н1}\ldots l_{в1}}$ и $S_{l_{н2}\ldots l_{в2}}$ ЭМЗАС-сети есть слой $S_{l_н\ldots l_в}=S_{l_{н1}\ldots l_{в1}}\cap S_{l_{н2}\ldots l_{в2}}$, где $l_н=\max(l_{н1},l_{н2})$, $l_в=\min(l_{в1},l_{в2})$, этой ЭМЗАС-сети, образованный такими и только такими уровнями ЭМЗАС, которые образуют одновременно оба из исходных слоев.

В сетевой трактовке понятия слоя ЭМЗАС-сети операции объединения и пересечения применимы только к пересекающимся слоям, а в системной – к любым. Например, результат объединения двух слоев может не быть слоем, тем не менее, такая операция в системной трактовке имеет смысл.

Суперблок $B_{l_н\ldots l_в}(I)$ *уровня* $l_в$ *с нижним уровнем* $l_н$ *и индексом* I (данный суперблок ЭМЗАС-сети имеет *порядок* $j = l_в - l_н + 1$ и *вписан в слой ЭМЗАС-сети* $S_{l_н\ldots l_в}$) *ЭМЗАС-сети* $B_0 = B_{1\ldots L}(0)$ – это (в сетевой трактовке) та часть слоя $S_{l_н\ldots l_в}$, индекс модулей которой $J \subseteq I$. Порядок суперблока имеет смысл количества уровней, на которых лежат его модули, уровень суперблока – наивысшего из этих уровней, а индекс суперблока – индекса единственного модуля уровня суперблока. Понятие суперблока обобщает понятия модуля $B_{l_в\ldots l_в}(I)$, блока $B_{l_в-1\ldots l_в}(I)$ и ЭМЗАС-сети в целом $B_0 = B_{1\ldots L}(0)$. Уровни ЭМЗАС, на которых лежат модули суперблока, можно поделить на три части: уровень суперблока, *нижний уровень суперблока* (самый нижний из этих уровней) и *средние уровни суперблока* (остальные из этих уровней). Модули, лежащие на этих уровнях, будем называть *верхними, нижними* и *средними модулями суперблока* соответственно. Обозначим через $Q_l(B)$, $P_l(B)$, $U_l(B)$ множества простых позиций l-го уровня, разрешающих позиций l-го уровня и модулей l-го уровня суперблока B, а через $Q(B) = \bigcup_{l=l_н}^{l_в} Q_l(B)$, $P(B) = \bigcup_{l=l_н}^{l_в} P_l(B)$, $U(B) = \bigcup_{l=l_н}^{l_в} U_l(B)$ – множества простых позиций, разрешающий позиций и модулей суперблока B.

Два суперблока ЭМЗАС-сети будем называть *пересекающимися*, если они имеют хотя бы один общий модуль, и *непересекающимися* в противном случае.

Теорема 1 (необходимое и достаточное условие пересечения суперблоков ЭМЗАС-сети). *Два суперблока ЭМЗАС-сети пересекаются тогда и только тогда, когда верхний модуль одного из них входит в состав другого.*

Следствие 1 из теоремы 1. *Различные суперблоки, вписанные в один и тот же слой, являются непересекающимися.*

Следствие 2 из теоремы 1. *Суперблоки одинакового уровня, но разного порядка либо являются непересекающимися, либо имеют общий верхний модуль и суперблок более высокого порядка содержит суперблок более низкого.*

Следствие 3 из теоремы 1. *Если различные суперблоки с одинаковым нижним уровнем являются пересекающимися, то они имеют разный порядок и суперблок более высокого порядка содержит в себе суперблок более низкого.*

Результат *пересечения двух пересекающихся суперблоков* ЭМЗАС-сети есть суперблок, модулями которого являются все общие модули исходных суперблоков. Данное определение предполагает, что общие модули любых пересекающихся суперблоков образуют новый суперблок. Это подтверждает следующая теорема.

Теорема 2. *Пусть* $B_{l_н\ldots l_в}(I) = B_{l_{н1}\ldots l_{в1}}(I_1) \cap B_{l_{н2}\ldots l_{в2}}(I_2)$. *Тогда выполнено:* $l_в = \min(l_{в1}, l_{в2})$, $l_н = \max(l_{н1}, l_{н2})$, *и если* $l_в = l_{в1}$, *то* $I = I_1$, *а если* $l_в = l_{в2}$, *то* $I = I_2$.

Исходной предпосылкой для формального задания ПБ на суперблоке ЭМЗАС-сети является тот факт, что суперблок j-го порядка L-уровневой ЭМЗАС-сети при изолированном его рассмотрении эквивалентен j-уровневой ЭМЗАС-сети. С этой точки зрения понятия ПБ на ЭМЗАС-сети естественно обобщаются на случай суперблоков.

Глобальная ПБ эталонной АСОД в смысле ЭМЗАС – это полномочия дискреционного доступа заданной авторизации к защищаемой информации как объектам уровня физических ресурсов АСОД (полномочия данного пользователя в данной роли по использованию физической среды хранения и передачи информации с учетом размещения конкретных элементов защищаемой информации). Ее математической моделью служит *глобальная ПБ на ЭМЗАС-сети*, которую на отдельном суперблоке $B = B_{l_н\ldots l_в}(I_0)$ будем задавать некоторым подмножеством разрешающих позиций нижнего уровня суперблока: $\Omega_г(B) \subseteq P_{l_н}(B)$. Позиции, входящие в множество $\Omega_г(B)$, назовем *позициями, разрешенными данной глобальной ПБ на суперблоке.*

Выполнение глобальной ПБ $\Omega_г(B)$ *на суперблоке* B ЭМЗАС-сети означает:

$$\left(\forall p = p[I,\alpha] \in P_{l_н}(B) \setminus \Omega_г(B)\right)\left(M_{вых}[I,\alpha] = 0\right), \quad (3)$$

т.е. все не разрешенные разрешающие позиции нижнего уровня не маркированы. Это интерпретируется как невозможность нелегального с точки зрения заданной ПБ дискреционного доступа к ресурсам нижнего уровня. *Нарушение (актуальное или потенциальное) глобальной ПБ* $\Omega_г(B)$ *на суперблоке* B ЭМЗАС-сети характеризуется актуальной или потенциальной маркированностью некоторой не разрешенной разрешающей позиции нижнего уровня, что интерпретируется как нелегальный для заданной ПБ дискреционный доступ к ресурсам нижнего уровня:

$$\left(\exists p = p[I,\alpha] \in P_{l_н}(B) \setminus \Omega_г(B)\right)\left(M_{вых}[I,\alpha] = 1\right). \quad (4)$$

Обобщением глобальной ПБ эталонной АСОД на произвольный уровень ЭМЗАС является *уровневая дискреционная ПБ эталонной АСОД* – 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* l*-го уровня на суперблоке* $B = B_{l_н \ldots l_в}(I_О)$, задаваемую множеством *разрешенных ею позиций* как подмножеством разрешающих позиций l-го уровня суперблока: $\Omega_{дl}(B) \subseteq P_l(B)$, $l_н \le l \le l_в$. Дискреционная ПБ нижнего уровня на суперблоке есть глобальная ПБ на нем.

Выполнение уровневой дискреционной ПБ $\Omega_{дl}(B)$ *на суперблоке* B означает:

$$\left(\forall p = p[I,\alpha] \in P_l(B) \setminus \Omega_{дl}(B)\right)\left(M_{вых}[I,\alpha] = 0\right), \quad (5)$$

т.е. все не разрешенные разрешающие позиции l-го уровня не маркированы. Это интерпретируется как невозможность осуществления дискреционного доступа к ресурсам данного уровня, нелегального с точки зрения заданной ПБ. *Нарушение (актуальное или потенциальное) уровневой дискреционной ПБ* $\Omega_{дl}(B)$ *на суперблоке* B ЭМЗАС-сети характеризуется актуальной или потенциальной маркированностью некоторой не разрешенной разрешающей позиции данного (l-го) уровня, что интерпретируется как нелегальный дискреционный доступ пользователя к объектам данного уровня:

$$\left(\exists p = p[I,\alpha] \in P_l(B) \setminus \Omega_{дl}(B)\right)\left(M_{вых}[I,\alpha] = 1\right). \quad (6)$$

Правила безопасного межсубъектного управления в эталонной АСОД 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 АСОД*), 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 суперблоке* $B = B_{l_н \ldots l_в}(I_О)$ ЭМЗАС-сети, задаваемую для l-го уровня множеством:

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

Такая ПБ устанавливает признаки допустимости авторизаций в модулях данного уровня данного суперблока (допустимость перемещения фишки из простой позиции в разрешающую для каждой пары противолежащих позиций данного уровня). Множество *позиций, разрешенных уровневой локальной ПБ* $\Omega_{лl}(B)$ на суперблоке B (разре-

шающие позиции данного уровня данного суперблока, в которые допустимо перемещение фишки) имеет вид:

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

Выполнение уровневой локальной ПБ $\Omega_{лl}(B)$ *на суперблоке* B означает:

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

т.е. никакая не разрешенная разрешающая позиция данного (l-го) уровня не может содержать фишку. Это интерпретируется как невозможность межсубъектного управления на данном уровне с нарушением предусмотренных ПБ уровневых правил безопасного межсубъектного управления. *Нарушение ПБ* $\Omega_{лl}(B)$ означает:

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

т.е. некоторая не разрешенная разрешающая позиция данного (l-го) уровня маркирована (интерпретируется как осуществление некоторого межсубъектного управления на данном уровне с нарушением предусмотренных ПБ уровневых правил).

Правила безопасного межсубъектного управления в эталонной АСОД декомпозируются также по управляющим субъектам. Математической моделью межсубъектного управления с фиксированным управляющим субъектом является блок ЭМЗАС-сети. Для произвольного блока 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 используется *блочная ПБ на ЭМЗАС-сети*, устанавливающая признаки допустимости всевозможных авторизаций во всех модулях данного блока (допустимость перемещения фишки 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 фишки) между верхним модулем, с одной стороны, и всеми нижними модулями, с другой. Предпосылкой согласования является одинаковая авторизация управляемого и управляющего субъектов в эталонной АСОД. На ЭМЗАС-сети это проявляется в том, что фишка 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:***

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

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

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 АСОД правил безопасного межсубъектного управления используется *локальная 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 на суперблоке $B = B_{l_н \ldots l_в}(I_0)$ можно множеством

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

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

Объединение по разным уровням отдельно первого и второго правил согласования признаков допустимости авторизации дает соответственно ***первое (13) и второе (14) правила согласования признаков допустимости авторизации при формальном задании локальной ПБ на суперблоке*** $B=B_{l_н\ldots l_в}(I_О)$**:**

$$\left(r[I,\alpha]=1\right)\Rightarrow\left(\forall J\subset I\middle|p[J,\alpha]\in P(B)\right)\left(r[J,\alpha]=1\right),\ \alpha=\overline{1,N},\ I=I(u),\ u\in U(B)\setminus U_{l_в}(B).\quad(13)$$

$$\left(r[I,\alpha]=0\right)\Rightarrow\left(\forall J\supset I\middle|p[J,\alpha]\in P(B)\right)\left(r[J,\alpha]=0\right),\ \alpha=\overline{1,N},\ I=I(u),\ u\in U(B)\setminus U_{l_н}(B).\quad(14)$$

Для математического моделирования согласованных по всей АСОД полномочий дискреционного доступа используется *дискреционная ПБ на ЭМЗАС-сети* как объединение уровневых дискреционных ПБ по всем уровням с их согласованием в рамках блочных ПБ. Задавать такую ПБ на суперблоке $B=B_{l_н\ldots l_в}(I_О)$ можно множеством

$$\Omega_{\partial p}(B)=\bigcup_{l=l_н}^{l_в}\Omega_{\partial l}(B)\subseteq P(B),\qquad(15)$$

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

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

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

Объединение по разным уровням правил (16) и (17) дает соответственно ***первое (18) и второе (19) правила согласования разрешенных позиций при формальном задании дискреционной ПБ на суперблоке*** $B=B_{l_н\ldots l_в}(I_О)$**:**

$$\left(p[I,\alpha]\in\Omega_{\partial p}(B)\right)\Rightarrow\left(\forall J\subset I\middle|p[J,\alpha]\in P(B)\right)\left(p[J,\alpha]\in\Omega_{\partial p}(B)\right),$$
$$\alpha=\overline{1,N},\ I=I(u),\ u\in U(B)\setminus U_{l_в}(B).\qquad(18)$$

$$\left(p[I,\alpha]\notin\Omega_{\partial p}(B)\right)\Rightarrow\left(\forall J\supset I\middle|p[J,\alpha]\in P(B)\right)\left(p[J,\alpha]\notin\Omega_{\partial p}(B)\right),$$
$$\alpha=\overline{1,N},\ I=I(u),\ u\in U(B)\setminus U_{l_н}(B).\qquad(19)$$

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

Разрешающее представление дискреционной ПБ на суперблоке 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* $\Omega_{\partial г}(B)$ *разрешенных позиций*, которое выразим через разрешающее представление $\Omega_{\partial p}(B)$ следующим образом:

$$\left(p[I,\alpha]\in\Omega_{\partial г}(B)\right)\Leftrightarrow\left(\left(p[I,\alpha]\in\Omega_{\partial p}(B)\right)\wedge\left(\forall J\supset I\middle|p[J,\alpha]\in P(B)\right)\left(p[J,\alpha]\notin\Omega_{\partial p}(B)\right)\right),$$

$$\alpha = \overline{1,N},\ I = I(u),\ u \in U(B). \qquad (20)$$

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

Теорема 3. *Разрешающее представление $\Omega_{др}(B)$ дискреционной ПБ на суперблоке B выражается через ее глобализованное представление $\Omega_{дг}(B)$:*

$$\left(p[I,\alpha] \in \Omega_{др}(B)\right) \Leftrightarrow \left(\left(\exists J \supseteq I \middle| p[J,\alpha] \in P(B)\right)\left(p[J,\alpha] \in \Omega_{дг}(B)\right)\right),$$

$$\alpha = \overline{1,N},\ I = I(u),\ u \in U(B). \qquad (21)$$

Теорема 4. *Пусть на суперблоке B ЭМЗАС-сети задана дискреционная ПБ с глобализованным представлением $\Omega_{дг}(B)$. Тогда имеет место формула:*

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

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

Теорема 5. *Всякое подмножество $\Omega_{дг}(B) \subset P(B)$ множества разрешающих позиций $P(B)$ суперблока B ЭМЗАС-сети, удовлетворяющее (22), однозначно задает на нем глобализованное представление некоторой дискреционной ПБ.*

Теорема 6 (существования и единственности глобализованного представления дискреционной ПБ на суперблоке ЭМЗАС-сети). *Любая дискреционная ПБ на суперблоке ЭМЗАС-сети имеет свое единственное глобализованное представление.*

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

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

т.е. все не разрешенные данной ПБ разрешающие позиции не маркированы (невозможность нелегального доступа). *Нарушение (актуальное или потенциальное) дискреционной ПБ на ЭМЗАС-сети* с разрешающим представлением $\Omega_{др}(B)$ характеризуется актуальной или потенциальной маркированностью не разрешенной разрешающей позиции (нелегальный доступ):

$$\left(\exists p = p[I,\alpha] \in P(B) \setminus \Omega_{др}(B)\right)\left(M_{вых}[I,\alpha] = 1\right). \qquad (24)$$

В эталонной АСОД гарантирование заданной дискреционной ПБ достигается поддержанием соответствующей (*индуцирующей ее*) локальной ПБ. Математической моделью этого является аналогичное индуцирование на ЭМЗАС-сети.

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

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

Так как согласование признаков допустимости авторизации эквивалентно согласованию разрешенных позиций, существует взаимно однозначное соответствие между ин-

дуцирующими локальными ПБ и индуцируемыми дискреционными ПБ.

Теорема 7 (основная теорема безопасности для дискреционной ПБ на суперблоке ЭМЗАС-сети). *Если в начальный момент времени выполняется заданная на некотором суперблоке ЭМЗАС-сети дискреционная ПБ, и все перемещения фишек на этом суперблоке удовлетворяют индуцирующей ее локальной ПБ, то в любой последующий момент времени эта дискреционная ПБ на суперблоке также выполняется.*

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

Назовем следующую *маркировку суперблока* $B = B_{l_н \ldots l_в}(I_0)$ *корневой*:

$$\left(\forall p = p[I,\alpha] \in P_{l_в}(B)\right)\left(\left(M_{вх}[I,\alpha]=1\right)\wedge\left(M_{вых}[I,\alpha]=0\right)\right)\wedge$$
$$\wedge\left(\forall p = p[I,\alpha] \in P(B)\setminus P_{l_в}(B)\right)\left(M_{вх}[I,\alpha]=M_{вых}[I,\alpha]=0\right), \qquad (26)$$

то есть все простые позиции уровня суперблока содержат фишку, но никакая из остальных позиций суперблока не содержит фишку. Корневая маркировка ЭМЗАС-сети в целом интерпретируется как отсутствие гиперпроцессов в эталонной АСОД.

Назовем следующую *маркировку суперблока B ЭМЗАС-сети индуцированной дискреционной ПБ с заданным глобализованным представлением* $\Omega_{дг}(B)$:

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

то есть все позиции из глобализованного множества разрешенных данной дискреционной ПБ позиций содержат фишку, но никакая из остальных позиций суперблока не содержит фишку. Такую маркировку суперблока ЭМЗАС-сети можно интерпретировать как реализацию дискреционного доступа к ресурсам его нижнего уровня с полномочиями, максимально предусмотренными заданной на суперблоке дискреционной ПБ.

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

Основные теоремы безопасности и достижимости для дискреционной ПБ на ЭМЗАС-сети в целом имеют естественную интерпретацию: для любой заданной дискреционной ПБ эталонной АСОД 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 нижнего уровня суперблока введем понятия индуцирования глобальной политики безопасности дискреционной и локальной политиками безопасности на суперблоке ЭМЗАС-сети.

Будем говорить, что заданная на суперблоке *B* ЭМЗАС-сети *дискреционная ПБ с глобализованным представлением* $\Omega_{дг}(B)$ *индуцирует на этом суперблоке глобальную ПБ* $\Omega_г(B)$, если $\Omega_г(B)=\Omega_{дг}(B)$.

В силу теоремы 5 всякое подмножество $\Omega_{дг}(B)\subset P(B)$ множества разрешающих позиций суперблока *B*, удовлетворяющее (22), однозначно задает на этом супер-

блоке глобализованное представление некоторой дискреционной ПБ. Подмножество $\Omega_g(B) \subset P(B)$ удовлетворяет (22), так как все его позиции относятся к одному (нижнему) уровню. Поэтому любая глобальная ПБ индуцируется единственной дискреционной ПБ на суперблоке. А она, в свою очередь, индуцируется некоторой локальной ПБ.

Будем говорить, что *заданная на некотором суперблоке локальная ПБ индуцирует на нем заданную глобальную ПБ*, если индуцирующая заданную глобальную ПБ дискреционная ПБ индуцируется заданной локальной ПБ.

Так как любая глобальная ПБ на суперблоке индуцируется единственной дискреционной ПБ на нем, а любая дискреционная ПБ индуцируется единственной локальной ПБ на этом же суперблоке, то любая глобальная ПБ индуцируется единственной локальной ПБ. Выполнение на суперблоке индуцирующей заданную глобальную ПБ дискреционной ПБ означает одновременно и выполнение заданной глобальной ПБ.

Теорема 9 (основная теорема безопасности для глобальной ПБ на суперблоке ЭМЗАС-сети). *Если в начальный момент времени выполняется индуцирующая заданную на суперблоке ЭМЗАС-сети глобальную ПБ дискреционная ПБ на нем, и все перемещения фишек удовлетворяют индуцирующей заданную глобальную ПБ локальной ПБ, то в любой последующий момент будет выполняться заданная глобальная ПБ.*

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

Теорема 10 (основная теорема достижимости для глобальной ПБ на суперблоке ЭМЗАС-сети). *Для любой заданной на суперблоке ЭМЗАС-сети глобальной ПБ всегда можно так определить разрешающие процедуры и процедуры преобразования на этом суперблоке, что индуцированная данной глобальной ПБ маркировка суперблока окажется достижимой из корневой его маркировки 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 АСОД однозначно определяются поддерживающие ее правила безопасного межсубъектного управления, при выполнении которых возможен легальный в рамках такой глобальной ПБ доступ и невозможен нелегальный.

При задании различных ПБ на различных суперблоках и ЭМЗАС-сети в целом может оказаться, что одни ПБ вступят в противоречие с другими. Тогда можно говорить о несовместимости некоторых ПБ. Прежде всего, необходимо формально определить возникающие в этой связи понятия совместимости и несовместимости. Будем различать сильную и слабую (в сильном и слабом смыслах) совместимость. Слабую будем понимать как отсутствие непосредственных противоречий, а сильную – еще и могущих возникнуть при распространении ПБ на всю ЭМЗАС-сеть. Для произвольных ПБ Ω_1 и Ω_2 их слабую совместимость будем обозначать $\Omega_1 \sim \Omega_2$, сильную – $\Omega_1 \approx \Omega_2$, слабую несовместимость – $\Omega_1 \not\sim \Omega_2$, сильную – $\Omega_1 \not\approx \Omega_2$. Несовместимость есть отсутствие соответствующей совместимости:

$$(\Omega_1 \not\sim \Omega_2) \Leftrightarrow \neg(\Omega_1 \sim \Omega_2);\ (\Omega_1 \not\approx \Omega_2) \Leftrightarrow \neg(\Omega_1 \approx \Omega_2).$$

Две произвольные ПБ будем называть *однотипными*, если они либо обе глобальные, либо обе уровневые дискреционные одного и того же уровня, либо обе уровневые локальные одного и того же уровня, либо обе локальные, либо обе дискреционные, и *разнотипными* в противном случае. Прежде всего, формально определим понятия *совместимости и несовместимости для однотипных ПБ*:

$$\left(\Omega_{г}(B_1)\sim\Omega_{г}(B_2)\right)\Leftrightarrow\left(\Omega_{г}(B_1)\cap P_{н}(B_2)=\Omega_{г}(B_2)\cap P_{н}(B_1)\right);$$

$$\left(\Omega_{г}(B_1)\not\sim\Omega_{г}(B_2)\right)\Leftrightarrow\left(\Omega_{г}(B_1)\cap P_{н}(B_2)\neq\Omega_{г}(B_2)\cap P_{н}(B_1)\right). \quad (28)$$

$$\left(\Omega_{\partial l}(B_1)\sim\Omega_{\partial l}(B_2)\right)\Leftrightarrow\left(\Omega_{\partial l}(B_1)\cap P_{l}(B_2)=\Omega_{\partial l}(B_2)\cap P_{l}(B_1)\right);$$

$$\left(\Omega_{\partial l}(B_1)\not\sim\Omega_{\partial l}(B_2)\right)\Leftrightarrow\left(\Omega_{\partial l}(B_1)\cap P_{l}(B_2)\neq\Omega_{\partial l}(B_2)\cap P_{l}(B_1)\right). \quad (29)$$

$$\left(\Omega_{лl}(B_1)\sim\Omega_{лl}(B_2)\right)\Leftrightarrow\left(\left|\Omega_{лl}(B_1)\cap\Omega_{лl}(B_2)\right|=N\cdot\left|U_{l}(B_1)\cap U_{l}(B_2)\right|\right);$$

$$\left(\Omega_{лl}(B_1)\not\sim\Omega_{лl}(B_2)\right)\Leftrightarrow\left(\left|\Omega_{лl}(B_1)\cap\Omega_{лl}(B_2)\right|<N\cdot\left|U_{l}(B_1)\cap U_{l}(B_2)\right|\right). \quad (30)$$

$$\left(\Omega_{л}(B_1)\sim\Omega_{л}(B_2)\right)\Leftrightarrow\left(\left|\Omega_{л}(B_1)\cap\Omega_{л}(B_2)\right|=N\cdot\left|U(B_1)\cap U(B_2)\right|\right);$$

$$\left(\Omega_{л}(B_1)\not\sim\Omega_{л}(B_2)\right)\Leftrightarrow\left(\left|\Omega_{л}(B_1)\cap\Omega_{л}(B_2)\right|<N\cdot\left|U(B_1)\cap U(B_2)\right|\right). \quad (31)$$

$$\left(\Omega_{\partial p}(B_1)\sim\Omega_{\partial p}(B_2)\right)\Leftrightarrow\left(\Omega_{\partial p}(B_1)\cap P(B_2)=\Omega_{\partial p}(B_2)\cap P(B_1)\right);$$

$$\left(\Omega_{\partial p}(B_1)\not\sim\Omega_{\partial p}(B_2)\right)\Leftrightarrow\left(\Omega_{\partial p}(B_1)\cap P(B_2)\neq\Omega_{\partial p}(B_2)\cap P(B_1)\right). \quad (32)$$

Из (28)-(32) видно, что слабая совместимость и несовместимость однотипных ПБ на одном и том же суперблоке означает их равенство и неравенство соответственно:

$$\left(\left(\Omega(B_1)\sim\Omega(B_2)\right)\wedge\left(B_1=B_2\right)\right)\Leftrightarrow\left(\Omega(B_1)=\Omega(B_2)\right);$$

$$\left(\left(\Omega(B_1)\not\sim\Omega(B_2)\right)\vee\left(B_1\neq B_2\right)\right)\Leftrightarrow\left(\Omega(B_1)\neq\Omega(B_2)\right). \quad (33)$$

Сильную совместимость однотипных ПБ будем понимать как их одновременную слабую совместимость с некоторой единой ПБ того же типа на всей ЭМЗАС-сети.

Таким образом, определение *сильной совместимости и несовместимости однотипных ПБ* $\Omega(B_1)$ и $\Omega(B_2)$ *на суперблоках* B_1 и B_2 ЭМЗАС-сети B_0:

$$\left(\Omega(B_1)\approx\Omega(B_2)\right)\Leftrightarrow\left(\left(\exists\Omega(B_0)\right)\left(\left(\Omega(B_1)\sim\Omega(B_0)\right)\wedge\left(\Omega(B_2)\sim\Omega(B_0)\right)\right)\right);$$

$$\left(\Omega(B_1)\not\approx\Omega(B_2)\right)\Leftrightarrow\left(\left(\forall\Omega(B_0)\right)\left(\left(\Omega(B_1)\not\sim\Omega(B_0)\right)\vee\left(\Omega(B_2)\not\sim\Omega(B_0)\right)\right)\right). \quad (34)$$

Из (34) видно, что слабая и, тем более, сильная совместимость и несовместимость однотипных ПБ на одном и том же суперблоке означает их равенство и неравенство:

$$\left(\left(\Omega(B_1)\sim\Omega(B_2)\right)\wedge\left(B_1=B_2\right)\right)\Leftrightarrow\left(\left(\Omega(B_1)\approx\Omega(B_2)\right)\wedge\left(B_1=B_2\right)\right)\Leftrightarrow\left(\Omega(B_1)=\Omega(B_2)\right);$$

$$\left(\left(\Omega(B_1)\not\sim\Omega(B_2)\right)\vee\left(B_1\neq B_2\right)\right)\Leftrightarrow\left(\left(\Omega(B_1)\not\approx\Omega(B_2)\right)\vee\left(B_1\neq B_2\right)\right)\Leftrightarrow\left(\Omega(B_1)\neq\Omega(B_2)\right). \quad (35)$$

Определим понятия совместимости и несовместимости для разнотипных ПБ.

Определение *слабой совместимости и несовместимости l-уровневой дискреционной ПБ* $\Omega_{\partial l}(B_1)$ *на суперблоке* B_1 *и дискреционной ПБ* с разрешающим представлением $\Omega_{\partial p}(B_2)$ *на суперблоке* B_2:

$$\left(\Omega_{\partial l}(B_1)\sim\Omega_{\partial p}(B_2)\right)\Leftrightarrow\left(\Omega_{\partial l}(B_1)\cap P(B_2)=\Omega_{\partial p}(B_2)\cap P_{l}(B_1)\right);$$

$$\left(\Omega_{\partial l}(B_1)\not\sim\Omega_{\partial p}(B_2)\right)\Leftrightarrow\left(\Omega_{\partial l}(B_1)\cap P(B_2)\neq\Omega_{\partial p}(B_2)\cap P_{l}(B_1)\right). \quad (36)$$

Слабую совместимость уровневых дискреционных ПБ разных уровней будем понимать как слабую совместимость некоторых дискреционных ПБ, с которыми данные уровневые дискреционные ПБ слабо совместимы (слабая совместимость уровневых дискреционных ПБ одинакового уровня получается как частный случай такой совместимости для разных уровней):

$$\left(\Omega_{\partial l_1}(B_1)\sim\Omega_{\partial l_2}(B_2)\right)\Leftrightarrow$$

$$\Leftrightarrow\left(\left(\exists\Omega_{\partial p}(B_1)\middle|\Omega_{\partial l_1}(B_1)\sim\Omega_{\partial p}(B_1)\right)\left(\exists\Omega_{\partial p}(B_2)\middle|\Omega_{\partial l_2}(B_2)\sim\Omega_{\partial p}(B_2)\right)\left(\Omega_{\partial p}(B_1)\sim\Omega_{\partial p}(B_2)\right)\right);$$

$$\left(\Omega_{\partial l_1}(B_1) \not\sim \Omega_{\partial l_2}(B_2)\right) \Leftrightarrow$$

$$\Leftrightarrow \left(\left(\forall \Omega_{\partial p}(B_1) \middle| \Omega_{\partial l_1}(B_1) \sim \Omega_{\partial p}(B_1)\right)\left(\forall \Omega_{\partial p}(B_2) \middle| \Omega_{\partial l_2}(B_2) \sim \Omega_{\partial p}(B_2)\right)\left(\Omega_{\partial p}(B_1) \not\sim \Omega_{\partial p}(B_2)\right)\right). \quad (37)$$

Определение *слабой совместимости и несовместимости l-уровневой локальной ПБ* $\Omega_{\text{л}l}(B_1)$ *на суперблоке* B_1 *и локальной ПБ* $\Omega_{\text{л}}(B_2)$ *на суперблоке* B_2:

$$\left(\Omega_{\text{л}l}(B_1) \sim \Omega_{\text{л}}(B_2)\right) \Leftrightarrow \left(\left|\Omega_{\text{л}l}(B_1) \cap \Omega_{\text{л}}(B_2)\right| = N \cdot \left|U_l(B_1) \cap U(B_2)\right|\right);$$

$$\left(\Omega_{\text{л}l}(B_1) \not\sim \Omega_{\text{л}}(B_2)\right) \Leftrightarrow \left(\left|\Omega_{\text{л}l}(B_1) \cap \Omega_{\text{л}}(B_2)\right| < N \cdot \left|U_l(B_1) \cap U(B_2)\right|\right). \quad (38)$$

Слабую совместимость уровневых локальных ПБ разных уровней будем понимать как слабую совместимость некоторых локальных ПБ, с которыми данные уровневые локальные ПБ слабо совместимы (слабая совместимость уровневых локальных ПБ одинакового уровня получается как частный случай слабой совместимости уровневых локальных ПБ разных уровней):

$$\left(\Omega_{\text{л}l_1}(B_1) \sim \Omega_{\text{л}l_2}(B_2)\right) \Leftrightarrow$$

$$\Leftrightarrow \left(\left(\exists \Omega_{\text{л}}(B_1) \middle| \Omega_{\text{л}l_1}(B_1) \sim \Omega_{\text{л}}(B_1)\right)\left(\exists \Omega_{\text{л}}(B_2) \middle| \Omega_{\text{л}l_2}(B_2) \sim \Omega_{\text{л}}(B_2)\right)\left(\Omega_{\text{л}}(B_1) \sim \Omega_{\text{л}}(B_2)\right)\right);$$

$$\left(\Omega_{\text{л}l_1}(B_1) \not\sim \Omega_{\text{л}l_2}(B_2)\right) \Leftrightarrow$$

$$\Leftrightarrow \left(\left(\forall \Omega_{\text{л}}(B_1) \middle| \Omega_{\text{л}l_1}(B_1) \sim \Omega_{\text{л}}(B_1)\right)\left(\forall \Omega_{\text{л}}(B_2) \middle| \Omega_{\text{л}l_2}(B_2) \sim \Omega_{\text{л}}(B_2)\right)\left(\Omega_{\text{л}}(B_1) \not\sim \Omega_{\text{л}}(B_2)\right)\right). \quad (39)$$

Взаимную слабую совместимость локальной, дискреционной и глобальной ПБ на одном и том же суперблоке будем понимать как индуцирование данной локальной ПБ данных дискреционной и глобальной и данной дискреционной ПБ данной глобальной. На основе этого можно определить соответствующие понятия слабой совместимости ПБ для пар различных суперблоков:

$$\left(\Omega_{\text{л}}(B_1) \sim \Omega_{\partial p}(B_2)\right) \Leftrightarrow \left(\left(\exists \Omega_{\partial p}(B_1) \middle| \Omega_{\text{л}}(B_1) \sim \Omega_{\partial p}(B_1)\right)\left(\Omega_{\partial p}(B_1) \sim \Omega_{\partial p}(B_2)\right)\right);$$

$$\left(\Omega_{\text{л}}(B_1) \not\sim \Omega_{\partial p}(B_2)\right) \Leftrightarrow \left(\left(\forall \Omega_{\partial p}(B_1) \middle| \Omega_{\text{л}}(B_1) \sim \Omega_{\partial p}(B_1)\right)\left(\Omega_{\partial p}(B_1) \not\sim \Omega_{\partial p}(B_2)\right)\right). \quad (40)$$

$$\left(\Omega_{\text{л}}(B_1) \sim \Omega_{\text{г}}(B_2)\right) \Leftrightarrow \left(\left(\exists \Omega_{\text{г}}(B_1) \middle| \Omega_{\text{л}}(B_1) \sim \Omega_{\text{г}}(B_1)\right)\left(\Omega_{\text{г}}(B_1) \sim \Omega_{\text{г}}(B_2)\right)\right);$$

$$\left(\Omega_{\text{л}}(B_1) \not\sim \Omega_{\text{г}}(B_2)\right) \Leftrightarrow \left(\left(\forall \Omega_{\text{г}}(B_1) \middle| \Omega_{\text{л}}(B_1) \sim \Omega_{\text{г}}(B_1)\right)\left(\Omega_{\text{г}}(B_1) \not\sim \Omega_{\text{г}}(B_2)\right)\right). \quad (41)$$

$$\left(\Omega_{\partial p}(B_1) \sim \Omega_{\text{г}}(B_2)\right) \Leftrightarrow \left(\left(\exists \Omega_{\text{г}}(B_1) \middle| \Omega_{\partial p}(B_1) \sim \Omega_{\text{г}}(B_1)\right)\left(\Omega_{\text{г}}(B_1) \sim \Omega_{\text{г}}(B_2)\right)\right);$$

$$\left(\Omega_{\partial p}(B_1) \not\sim \Omega_{\text{г}}(B_2)\right) \Leftrightarrow \left(\left(\forall \Omega_{\text{г}}(B_1) \middle| \Omega_{\partial p}(B_1) \sim \Omega_{\text{г}}(B_1)\right)\left(\Omega_{\text{г}}(B_1) \not\sim \Omega_{\text{г}}(B_2)\right)\right). \quad (42)$$

Слабую совместимость уровневой локальной и уровневой дискреционной ПБ будем понимать как слабую совместимость некоторых локальной и дискреционной ПБ, с которыми данные ПБ соответственно слабо совместимы:

$$\left(\Omega_{\text{л}l_1}(B_1) \sim \Omega_{\partial l_2}(B_2)\right) \Leftrightarrow$$

$$\Leftrightarrow \left(\left(\exists \Omega_{\text{л}}(B_1) \middle| \Omega_{\text{л}l_1}(B_1) \sim \Omega_{\text{л}}(B_1)\right)\left(\exists \Omega_{\partial p}(B_2) \middle| \Omega_{\partial l_2}(B_2) \sim \Omega_{\partial p}(B_2)\right)\left(\Omega_{\text{л}}(B_1) \sim \Omega_{\partial p}(B_2)\right)\right);$$

$$\left(\Omega_{\text{л}l_1}(B_1) \not\sim \Omega_{\partial l_2}(B_2)\right) \Leftrightarrow$$

$$\Leftrightarrow \left(\left(\forall \Omega_{\text{л}}(B_1) \middle| \Omega_{\text{л}l_1}(B_1) \sim \Omega_{\text{л}}(B_1)\right)\left(\forall \Omega_{\partial p}(B_2) \middle| \Omega_{\partial l_2}(B_2) \sim \Omega_{\partial p}(B_2)\right)\left(\Omega_{\text{л}}(B_1) \not\sim \Omega_{\partial p}(B_2)\right)\right). \quad (43)$$

Слабую совместимость уровневой локальной и дискреционной ПБ будем понимать как слабую совместимость данной дискреционной ПБ с некоторой локальной ПБ, с которой данная уровневая локальная ПБ слабо совместима:

$$\left(\Omega_{лl}(B_1)\sim\Omega_{\partial p}(B_2)\right)\Leftrightarrow\left(\left(\exists\Omega_{л}(B_1)\middle|\Omega_{лl}(B_1)\sim\Omega_{л}(B_1)\right)\left(\Omega_{л}(B_1)\sim\Omega_{\partial p}(B_2)\right)\right);$$

$$\left(\Omega_{лl}(B_1)\not\sim\Omega_{\partial p}(B_2)\right)\Leftrightarrow\left(\left(\forall\Omega_{л}(B_1)\middle|\Omega_{лl}(B_1)\sim\Omega_{л}(B_1)\right)\left(\Omega_{л}(B_1)\not\sim\Omega_{\partial p}(B_2)\right)\right). \qquad (44)$$

Слабую совместимость уровневой локальной и глобальной ПБ будем понимать как слабую совместимость данной глобальной ПБ с некоторой локальной ПБ, с которой данная уровневая локальная ПБ слабо совместима:

$$\left(\Omega_{лl}(B_1)\sim\Omega_{г}(B_2)\right)\Leftrightarrow\left(\left(\exists\Omega_{л}(B_1)\middle|\Omega_{лl}(B_1)\sim\Omega_{л}(B_1)\right)\left(\Omega_{л}(B_1)\sim\Omega_{г}(B_2)\right)\right);$$

$$\left(\Omega_{лl}(B_1)\not\sim\Omega_{г}(B_2)\right)\Leftrightarrow\left(\left(\forall\Omega_{л}(B_1)\middle|\Omega_{лl}(B_1)\sim\Omega_{л}(B_1)\right)\left(\Omega_{л}(B_1)\not\sim\Omega_{г}(B_2)\right)\right). \qquad (45)$$

Слабую совместимость уровневой дискреционной и локальной ПБ будем понимать как слабую совместимость данной локальной ПБ с некоторой дискреционной ПБ, с которой данная уровневая дискреционная ПБ слабо совместима:

$$\left(\Omega_{\partial l}(B_1)\sim\Omega_{л}(B_2)\right)\Leftrightarrow\left(\left(\exists\Omega_{\partial p}(B_1)\middle|\Omega_{\partial l}(B_1)\sim\Omega_{\partial p}(B_1)\right)\left(\Omega_{\partial p}(B_1)\sim\Omega_{л}(B_2)\right)\right);$$

$$\left(\Omega_{\partial l}(B_1)\not\sim\Omega_{л}(B_2)\right)\Leftrightarrow\left(\left(\forall\Omega_{\partial p}(B_1)\middle|\Omega_{\partial l}(B_1)\sim\Omega_{\partial p}(B_1)\right)\left(\Omega_{\partial p}(B_1)\not\sim\Omega_{л}(B_2)\right)\right). \qquad (46)$$

Слабую совместимость уровневой дискреционной и глобальной ПБ будем понимать как слабую совместимость данной глобальной ПБ с некоторой дискреционной ПБ, с которой данная уровневая дискреционная ПБ слабо совместима:

$$\left(\Omega_{\partial l}(B_1)\sim\Omega_{г}(B_2)\right)\Leftrightarrow\left(\left(\exists\Omega_{\partial p}(B_1)\middle|\Omega_{\partial l}(B_1)\sim\Omega_{\partial p}(B_1)\right)\left(\Omega_{\partial p}(B_1)\sim\Omega_{г}(B_2)\right)\right);$$

$$\left(\Omega_{\partial l}(B_1)\not\sim\Omega_{г}(B_2)\right)\Leftrightarrow\left(\left(\forall\Omega_{\partial p}(B_1)\middle|\Omega_{\partial l}(B_1)\sim\Omega_{\partial p}(B_1)\right)\left(\Omega_{\partial p}(B_1)\not\sim\Omega_{г}(B_2)\right)\right). \qquad (47)$$

Сильную совместимость разнотипных ПБ на суперблоках будем понимать как слабую совместимость некоторых ПБ тех же типов на всей ЭМЗАС-сети, которые слабо совместимы с соответствующими исходными ПБ на суперблоках (сильная совместимость однотипных ПБ на суперблоках (34) получается как частный случай сильной совместимости разнотипных ПБ на суперблоках):

$$\left(\Omega_1(B_1)\approx\Omega_2(B_2)\right)\Leftrightarrow$$

$$\Leftrightarrow\left(\left(\exists\Omega_1(B_0)\middle|\Omega_1(B_1)\sim\Omega_1(B_0)\right)\left(\exists\Omega_2(B_0)\middle|\Omega_2(B_2)\sim\Omega_2(B_0)\right)\left(\Omega_1(B_0)\sim\Omega_2(B_0)\right)\right);$$

$$\left(\Omega_1(B_1)\not\approx\Omega_2(B_2)\right)\Leftrightarrow$$

$$\Leftrightarrow\left(\left(\forall\Omega_1(B_0)\middle|\Omega_1(B_1)\sim\Omega_1(B_0)\right)\left(\forall\Omega_2(B_0)\middle|\Omega_2(B_2)\sim\Omega_2(B_0)\right)\left(\Omega_1(B_0)\not\sim\Omega_2(B_0)\right)\right). \qquad (48)$$

Номера формул, определяющих слабую и сильную совместимость и несовместимость ПБ на суперблоках ЭМЗАС-сети, сведем в таблицу 1 с символическими обозначениями ПБ: Г – глобальная, УД – уровневая дискреционная, УЛ – уровневая локальная, Л – локальная, Д – дискреционная.

Таблица 1

Номера формул совместимости ПБ на суперблоках ЭМЗАС-сети

ПБ	Г	УД	УЛ	Л	Д
Г	(28), (34)	(47), (48)	(45), (48)	(41), (48)	(42), (48)
УД		(29), (37), (34), (48)	(43), (48)	(46), (48)	(36), (48)
УЛ			(30), (39), (34), (48)	(38), (48)	(44), (48)
Л				(31), (34)	(40), (48)
Д					(32), (34)

Теорема 11 (о соотношении слабой и сильной совместимости ПБ на суперблоках ЭМЗАС-сети). *Пусть* $\Omega_1(B_1)$ *и* $\Omega_2(B_2)$ *– в общем случае разнотипные ПБ на суперблоках* B_1 *и* B_2 *с индексами* $I_1 = I(B_1)$ *и* $I_2 = I(B_2)$ *соответственно. Тогда возможны следующие случаи.*

1. Суперблоки пересекающиеся. Тогда слабая и сильная совместимость ПБ эквивалентны: $(\Omega_1(B_1) \sim \Omega_2(B_2)) \Leftrightarrow (\Omega_1(B_1) \approx \Omega_2(B_2))$. *Если при этом суперблоки совпадают* $(B_1 = B_2 = B)$ *и ПБ однотипные, то слабая и сильная их совместимость эквивалентна их равенству:* $(\Omega_1(B) \sim \Omega_2(B)) \Leftrightarrow (\Omega_1(B) \approx \Omega_2(B)) \Leftrightarrow (\Omega_1(B) = \Omega_2(B))$.

2. Суперблоки непересекающиеся, но индекс одного из них является подиндексом индекса другого: $I_2 \subset I_1$. *Тогда данные ПБ обязательно слабо совместимы, но необязательно сильно совместимы.*

3. Индекс ни одного из суперблоков не является подиндексом индекса другого: $(I_1 \not\subset I_2) \wedge (I_2 \not\subset I_1)$. *Тогда данные ПБ обязательно сильно и, тем более, слабо совместимы.*

Будем говорить, что *на суперблоке B ЭМЗАС-сети задан комплекс ПБ* $\Omega(B)$, если на этом суперблоке определены ПБ всех типов, и *задан корректно*, если все эти ПБ взаимно совместимы (здесь совместимость в сильном и слабом смыслах эквивалентны). Комплекс ПБ на суперблоке *B* ЭМЗАС-сети можно представлять следующим кортежем:

$$\Omega(B) = \langle \Omega_г(B), \Omega_{др}(B), \Omega_{дг}(B), \Omega_л(B) \rangle, \qquad (49)$$

где $\Omega_г(B)$ и $\Omega_л(B)$ – глобальная и локальная ПБ, а $\Omega_{др}(B)$ и $\Omega_{дг}(B)$ – разрешающее и глобализованное представления дискреционной ПБ. Существование локальной и дискреционной ПБ предполагает согласованность в их рамках уровневых локальных и уровневых дискреционных ПБ. Корректность задания комплекса ПБ (49) означает, что дискреционная ПБ индуцирована локальной, а глобальная – локальной и дискреционной. *Совместимость* или *несовместимость в сильном* или *слабом смысле корректно заданных комплексов ПБ* на суперблоках будем понимать как соответственно наличие или отсутствие взаимной совместимости в сильном или слабом смысле всех ПБ на этих суперблоках. Таким образом, комплексы ПБ на суперблоках ЭМЗАС-сети моделируют комплексы ПБ подсистем эталонных АСОД с использованием естественных понятий корректности и совместимости.

Математические модели регламентируемых ЭМЗАС комплексов ПБ рассмотрены с более общих позиций, предусматривающих возможность их задания лишь на некоторой подсистеме эталонной АСОД. Для всех приведенных утверждений разработаны доказательства, которые пришлось опустить ввиду ограниченности объема статьи. Вместо рассматриваемых ранее комплексов ПБ на ЭМЗАС-сети исследуются комплексы ПБ на отдельном произвольно заданном ее суперблоке. Если в качестве суперблока взять всю ЭМЗАС-сеть, то все полученные в данной работе результаты полностью совпадут с результатами для ЭМЗАС-сети в целом, полученными в [1]. Однако проведенное обобщение направлено, в конечном итоге, на расширение возможностей разработки АСОД КП, так как создает базу *послойного синтеза ПБ на ЭМЗАС-сети* как синтеза комплекса ПБ на ЭМЗАС-сети в целом по подходящим образом выбранному ее конечному разложению на множества суперблоков. При этом ключевое значение приобретает рассмотренный в данной работе вопрос обеспечения совместимости ПБ, заданных на различных суперблоках. Способы проведения конечных разложений ЭМЗАС-сети определяются заданием на ней соответствующих полуколец множеств. В

качестве примера такого полукольца множеств на ЭМЗАС-сети можно привести полукольцо $\{\varnothing; B_0; B_{10\ldots13}(o); B_{7\ldots9}(I(u))|u \in U_9; B_{1\ldots6}(I(u))|u \in U_6\}$ слоисто-суперблочной структуры ЭМЗАС-сети, заданной ее разбиением на смежные слои $\{S_{1\ldots6}, S_{7\ldots9}, S_{10\ldots13}\}$. Приведенное полукольцо можно использовать при послойном синтезе с использованием ПБ на суперблоках, моделирующих СУБД. Вообще же, возможность послойного синтеза ПБ на ЭМЗАС-сети существенно расширяет теоретические предпосылки для реализации ЭМЗАС в практике разработки АСОД КП.

Литература

1. Дубровин, А. С. Математическая модель политики безопасности эталонной автоматизированной системы на основе ЭМЗАС-сети [Текст] / А. С. Дубровин, В. И. Сумин, М. В. Коротков, А. Ю. Немченко // Вестник ВГУ. Сер. Физика. Математика. – Воронеж : Воронеж. гос. ун-т, 2005. – № 2. – С. 147–155.

2. Дубровин, А. С. Слоистая структура ЭМЗАС-сети [Текст] / А. С. Дубровин, В. И. Сумин, С. В. Родин, Г. В. Перминов // Вестник Воронежского института МВД России. – Воронеж : Воронеж. ин-т МВД России, 2007. – № 1. – С. 153–158.

3. Герасименко, В. Г. Проблемы обеспечения информационной безопасности при использовании открытых информационных технологий в системах критических приложений [Текст] / В. Г. Герасименко // Информация и безопасность : региональный науч.-технический вестник. – Воронеж : Воронеж. гос. техн. ун-т, 1999. – Вып. 4. – С. 66–67.

4. Дубровин, А. С. Информационная безопасность и защита информации в экономических информационных системах [Текст] : учеб. пособие / А. С. Дубровин, М. Г. Матвеев, Е. А. Рогозин, В. И. Сумин. – Воронеж : Воронеж. гос. технол. акад., 2005. – 292 с.

5. Сумин, В. И. Эталонная модель защищенной автоматизированной системы [Текст] / В. И. Сумин, А. С. Дубровин // Материалы международной науч.-практической конф. «Информационно-аналитическое обеспечение раскрытия и расследования преступлений правоохранительными органами», 24–25 мая 2007 г. – Белгород : Белгород. юр. ин-т МВД России, 2007. – С. 52–58.

6. Девянин, П. Н. Модели безопасности компьютерных систем [Текст] : учеб. пособие для студ. высш. учеб. заведений / П. Н. Девянин. – М. : Издательский центр «Академия», 2005. – 144 с.

7. Щербаков, А. Ю. Введение в теорию и практику компьютерной безопасности [Текст] / А. Ю. Щербаков. – М. : Молгачева С. В., 2001. – 352 с.

8. Костин, А. Е. Организация и обработка структур данных в вычислительных системах [Текст] : учеб. пособие для вузов / А. Е. Костин, В. Ф. Шаньгин. – М. : Высш. шк., 1987. – 248 с.

REFERENCE DATA PROCESSING SYSTEM SUBSYSTEM SECURITY POLICY MATHEMATICAL MODEL ON THE PSSM-NETWORK BASIS

A.S. Dubrovin [1]
V.I. Sumin [2]

[1] *Voronezh State Technological Academy*

[2] *Voronezh Institute of the Ministry of Internal Affairs of Russia*

e-mail: asd_kiziltash@box.vsi.ru

Mathematical models by regulated of the protected system standard model (PSSM) security policies (SP) a separate subsystem of the data processing system (DPS) are constructed on the basis of a means of PSSM-networks. The constructed models give a basis for synthesis reference DPS SP on subsystems, that essentially expands theoretical premises for PSSM realization in practice of critical application DPS development.

Keywords: protected system standard model (PSSM), critical application data processing system (DPS), discretionary access, basic theorem of safety, superblock of the PSSM-networks.