МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.94

МНОГОУРОВНЕВОЕ ТЕМАТИКО-ИЕРАРХИЧЕСКОЕ УПРАВЛЕНИЕ ДОСТУПОМ (MLTHS-СИСТЕМА)

Н. А. Гайдамакин

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург, Россия

Управление доступом строится на объединении доверительно-мандатного и тематического принципа. Субъектам и объектам доступа присваиваются составные метки безопасности, содержащие уровень безопасности (гриф секретности для объектов, уровень допуска для субъектов) и тематический индекс (тематика объектов, тематические полномочия субъектов). В отличие от известной MLS-модели, использующей неиерархические, т. е. неупорядоченные, тематические категории в виде набора тематических рубрик, тематические индексы объектов и тематические полномочия субъектов отображаются элементами иерархических тематических классификаторов, которые широко применяются в технологиях организации документальных хранилищ. Математически метки безопасности представляют собой элементы произведения линейной решётки уровней безопасности, применяемой в модели Белла — ЛаПадулы, и специально построенной решётки мультирубрик на иерархических классификаторах. Построены специальные отношения доминирования («шире — уже»), операции взятия наименьшей верхней и наибольшей нижней границ мультирубрик, которые не могут быть выражены обычными теоретико-множественными отношениями включения, операциями объединения и пересечения. В MLTHS-системе определены процедуры присвоения пользователям и инициируемым ими субъектам меток безопасности. Установлены правила санкционирования монитором безопасности доступов субъектов к объектам на чтение, запись, выполнение, в том числе определены процедуры присвоения меток безопасности вновь создаваемым объектам. Установлены правила санкционирования множественных доступов (одного субъекта одновременно к нескольким объектам, нескольких субъектов одновременно к одному объекту). Доказывается безопасность функционирования MLTHS-системы по критерию отсутствия потоков «сверху вниз» и между несравнимыми по меткам безопасности сущностями (субъектами или объектами доступа). MLTHS-система позволяет соединить технологии текстового поиска в документальных хранилищах и технологии разграничения доступа, создавая на этой основе защищённые документально-поисковые системы без ограничения их функциональности.

Ключевые слова: *управление доступом, модель безопасности, иерархический тематический классификатор, мультирубрика, решётка мультирубрик, документальные информационно-поисковые системы, тематическое индексирование, MLS-модель.*

DOI 10.17223/20710410/39/4

MULTILEVEL THEMATIC-HIERARCHICAL ACCESS CONTROL (MLTHS-SYSTEM)

N. A. Gaydamakin

Ural Federal University, Ekaterinburg, Russia

E-mail: haid2@bk.ru

Access control in computer systems is based on the combination of confidence-mandatory and thematic principles. Composite security labels (tags) containing a security level (classification grade for objects and access level for subjects) and a thematic index (object themes and thematic permissions for subjects) are assigned to the access objects and subjects. In contrast to the known MLS-model that uses so called non-hierarchical (i.e. unordered) thematic categories in the form of thematic rubrics, our model (MLTS-system) uses thematic object indexes and thematic subject permissions which appear as hierarchical thematic classifier elements widely used in document storage technologies. Mathematically, the security labels are elements of the product of the security level algebraic lattice used in Bell — LaPadula model and of a special multirubric lattice based on hierarchical classifiers. Special dominance relations (wider — narrower) and binary operations (greatest lower and least upper multirubric bounds) that cannot be expressed by using ordinary set-theoretic inclusion relation and union and intersection operations are introduced. In MLTHS-system, for assigning security tags to users and to user-initiated subjects, some specific procedures are defined. Authorization rules to subject-to-object read, write and execute access are defined for security monitor as well as security tag assignment procedures for newly created objects. Multiple access (a single subject to many objects and many subjects to a single object) authorization rules are established. It is proven that MLTHS-system is secure by criteria of flow absence between security tag-incomparable entities (objects or subjects) and of top down flow absence. MLTHS-system allows combining access control and document storage text search technologies to create secure search engines with no functional limitations.

Keywords: *access control (management), security model, hierarchical thematic classifier, multirubric, multirubric lattice, documentary information retrieval systems, thematic indexing, MLS-model.*

1. Исходные положения

Широко известным подходом к управлению доступом к информационным объектам в компьютерных системах (КС) является применение мандатной политики [1 – 3]. Реализующая эту политику модель Белла — ЛаПадулы [4] основывается на линейной решётке неких абстрактных уровней безопасности

$$\Lambda_{\mathsf{L}}(L, <, \circ, \otimes),$$

где L — множество уровней безопасности; $<$ — отношение доминирования, определяющее строгий и полный порядок на множестве L; $\circ$ — оператор, определяющий для любой пары $l_1, l_2 \in L$ точную (наименьшую) верхнюю границу $l = l_1 \circ l_2 = \max(l_1, l_2)$; $\otimes$ — оператор, определяющий для любой пары $l_1, l_2 \in L$ точную (наибольшую) нижнюю границу $l = l_1 \otimes l_2 = \min(l_1, l_2)$.

Множество сущностей системы управления доступом (множество субъектов доступа $s \in S$ и множество объектов доступа $o \in O$) отображаются на решётку уровней безопасности Λ_{L}. Результатом отображения (классификации) является присвоение каждому субъекту или объекту уровня безопасности, который для субъектов именуется уровнем допуска, а для объектов — грифом секретности.

Критерием безопасности является запрет информационных потоков «сверху вниз», т. е. от сущностей с более высоким уровнем безопасности к сущностям с более низким уровнем безопасности.

Вместе с тем «подсмотренная» в сфере традиционного «бумажного» секретного делопроизводства политика мандатного управления доступом на основе грифов секретности и уровней допуска не является единственной. В специальных библиотеках, в архивах многих организаций и предприятий управление доступом осуществляется по тематическому принципу, т. е. в зависимости от тематики сведений, находящихся в информационных объектах. Наиболее простой подход основан на решётке множества подмножеств тематических категорий (тематических рубрик):

$$\Lambda_{\mathsf{TD}}(\boldsymbol{P}_{\mathsf{TD}}, \subseteq, \cup, \cap),$$

где $\boldsymbol{P}_{\mathsf{TD}}$ — множество подмножеств P_{TD} из базового множества тематических категорий $T_{\mathsf{TD}} = \{\tau_1, \tau_2, \dots\}$; τ_i — i-я тематическая категория (рубрика); $P_{\mathsf{TD}} \in \boldsymbol{P}_{\mathsf{TD}}$; $P_{\mathsf{TD}} \subseteq T_{\mathsf{TD}}$; $\subseteq$ — отношение теоретико-множественного включения, определяющее на множестве $\boldsymbol{P}_{\mathsf{TD}}$ отношение нестрого частичного порядка; $\cup$ — операция теоретико-множественного объединения, определяющая для любой пары $P_{\mathsf{TD}1}, P_{\mathsf{TD}2} \in \boldsymbol{P}_{\mathsf{TD}}$ наименьшую верхнюю границу $P_{\mathsf{TD}\cup} = P_{\mathsf{TD}1} \cup P_{\mathsf{TD}2}$; $\cap$ — операция теоретико-множественного пересечения, определяющая для любой пары $P_{\mathsf{TD}1}, P_{\mathsf{TD}2} \in \boldsymbol{P}_{\mathsf{TD}}$ наибольшую нижнюю границу $P_{\mathsf{TD}\cap} = P_{\mathsf{TD}1} \cap P_{\mathsf{TD}2}$.

Критерием безопасности является недопустимость информационных потоков от сущностей с более широкой тематикой к сущностям с более узкой тематикой, а также между несравнимыми по отношению включения сущностями.

Поскольку в некоторых областях, в частности в области обработки текстов, набор элементов, характеризующих тематику информационных объектов (набор ключевых слов, набор тематических рубрик), называют дескрипторами, то $\Lambda_{\mathsf{TD}}(\boldsymbol{P}_{\mathsf{TD}}, \subseteq, \cup, \cap)$ будем называть *дескрипторной тематической решёткой*.

На рис. 1 представлены диаграмма Хассе решётки $\Lambda_{\mathsf{TD}}(\boldsymbol{P}_{\mathsf{TD}}, \subseteq, \cup, \cap)$ на множестве из трёх тематических рубрик $T_{\mathsf{TD}} = \{\tau_1, \tau_2, \tau_3\}$ и граф допустимых по критерию «снизу вверх» потоков. Символ $\varnothing$ соответствует «пустой» рубрике, т. е., в контексте управления доступом, такой тематике сведений, доступ к которым неограничен.

Пунктирные стрелки на рис. 1, *б* задают допустимые информационные потоки между сущностями с соответствующими тематическими категориями. Все остальные потоки являются недопустимыми как потоки от сущностей с более широкой тематикой к сущностям с более узкой тематикой или как потоки между несравнимыми по тематике сущностями.

При объединении рассмотренных подходов субъекты и объекты доступа отображаются в произведение решёток $\Lambda_{\mathsf{L}}(L, <, \circ, \otimes)$ и $\Lambda_{\mathsf{TD}}(\boldsymbol{P}_{\mathsf{TD}}, \subseteq, \cup, \cap)$. Каждый субъект или объект доступа помечается двойной меткой: уровнем секретности и тематическим индексом в виде набора тематических («неиерархических») категорий.

На рис. 2 представлен результат произведения линейной решётки из двух уровней безопасности $(l_1, l_2; l_1 < l_2)$ и тематической решётки из двух рубрик $\{\tau_1, \tau_2\}$.

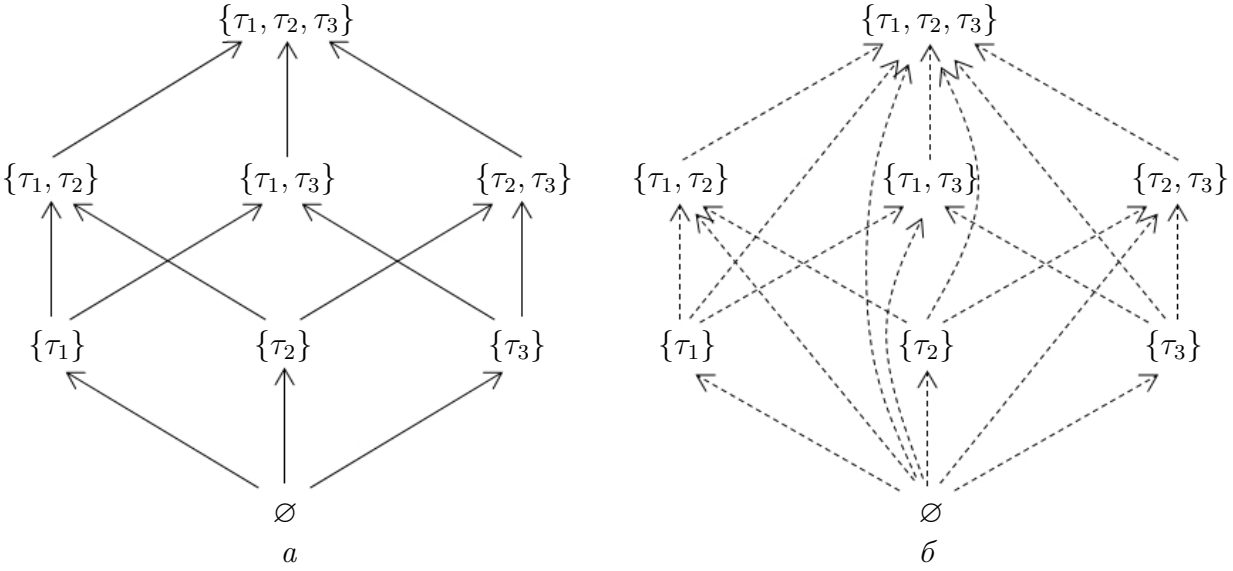


Рис. 1. Диаграмма Хассе решётки подмножеств на множестве из трёх тематических рубрик $\{\tau_1, \tau_2, \tau_3\}$ (*а*) и граф допустимых потоков в системе управления доступом (*б*)

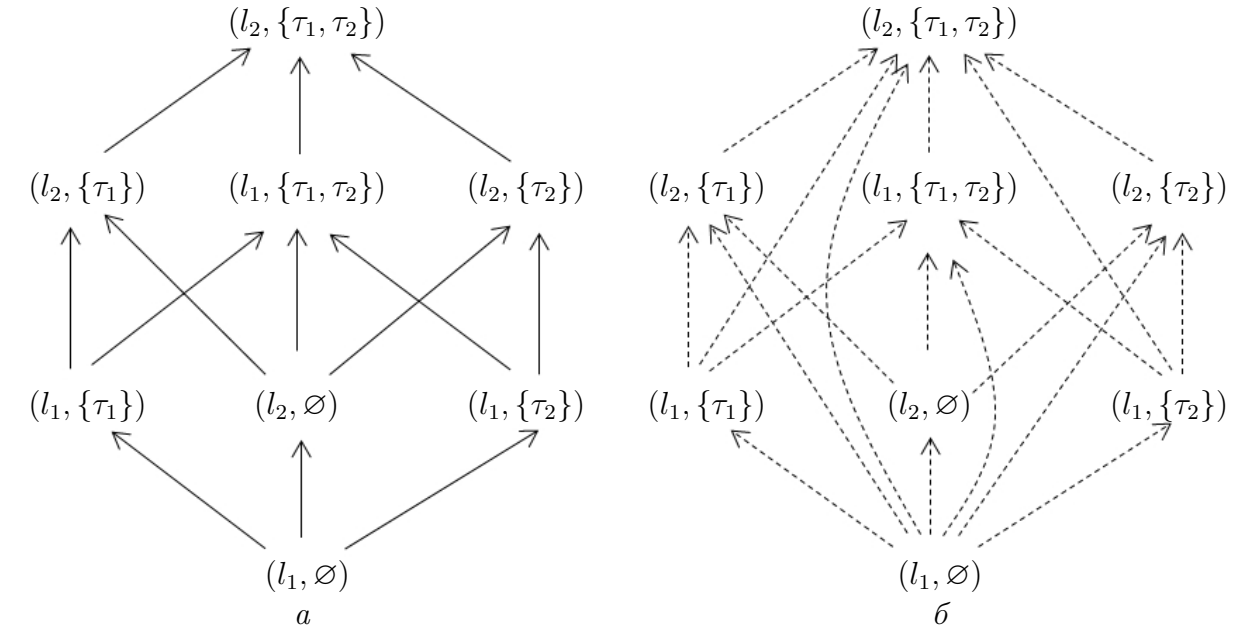


Рис. 2. Диаграмма Хассе произведения линейной решётки из двух уровней безопасности $(l_1, l_2; l_1 < l_2)$ и тематической решётки из двух рубрик $\{\tau_1, \tau_2\}$ (*а*) и граф допустимых потоков (*б*)

Объединённый подход, именуемый в некоторых источниках как *MLS-модель*[1], позволяет строить системы управления доступом, отражающие существенно более разнообразные технологии работы с конфиденциальной информацией, более адекватно настраиваемые на особенности информационно-технологической сферы конкретных организаций.

[1]Multi-Level Security. В некоторых источниках под термином MLS понимают в целом модели мандатной политики, в том числе модель Белла — ЛаПадулы, характеризующиеся наличием множества уровней безопасности.

Вместе с тем в MLS-модели, как и в базовой модели Белла — ЛаПадулы, не определены такие важные в практической реализации аспекты, как присвоение/изменение уровней безопасности и тематических меток субъектам и объектам доступа, процедуры совместного доступа субъектов к какому-либо объекту, одновременного доступа субъекта к нескольким объектам.

Кроме того, в технологиях текстового поиска при организации хранилищ документов широко применяется индексирование текстовых документов не просто наборами тематических рубрик (ключевых слов), а элементами иерархически-организованных классификационных структур (иерархические тематические классификаторы, тезаурусы, иерархические онтологии [5]), использование которых не может быть отражено с помощью простой дескрипторной тематической решётки $\Lambda_{\mathsf{TD}}(\boldsymbol{P}_{\mathsf{TD}}, \subseteq, \cup, \cap)$.

В [6] представлена модель тематического разграничения доступа при иерархической структуре классификатора, введено понятие мультирубрики и построена решётка мультирубрик. Приведём в кратком изложении основные положения алгебры мультирубрик.

2. Мультирубрики и решётка мультирубрик на иерархическом тематическом классификаторе

Иерархические тематические классификаторы, применяемые для тематического индексирования информационных объектов (книг в библиотеках, документов в делопроизводстве), строятся по таксономическому (родовидовому) принципу. Вся тематика предметной области разбивается на рубрики, которые, в свою очередь, могут разбиваться на подрубрики и т. д. Таким образом, если сведения, содержащиеся в информационном объекте, отнесены к рубрике τ_i, то в нём содержатся сведения по всем подрубрикам τ_j, составляющим рубрику τ_i, т. е. подчинённым рубрике τ_i.

В теоретико-множественной интерпретации иерархический тематический классификатор представляет собой частично упорядоченное множество тематических категорий (рубрик) $T_{\mathsf{TH}} = \{\tau_1, \tau_2, \ldots, \tau_K\}$, образующих корневое дерево (см., например, рис. 3).

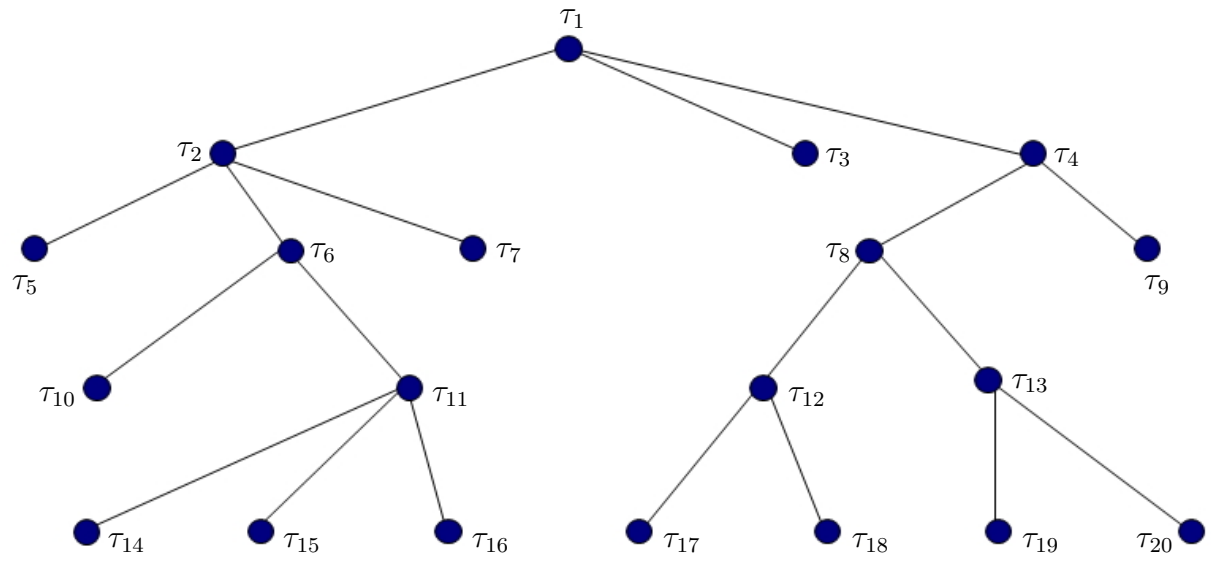


Рис. 3. Пример иерархического тематического классификатора в виде корневого графа (τ_1 — корень дерева, обозначающий всю тематику предметной области)

Информационный объект может содержать сведения, относящиеся сразу к нескольким рубрикам. С учётом иерархической сущности классификатора для тематического индексирования информационных объектов вводится понятие «*мультирубрика*».

Определение 1. Мультирубрикой $\mathcal{T}_i^{\mathsf{M}}$ называется любое подмножество $\{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_L}\}$ $(L \leqslant K)$ множества $T_{\mathsf{TH}} = \{\tau_1, \tau_2, \ldots, \tau_K\}$ рубрик-вершин иерархического тематического классификатора, такое, что:

а) любая вершина τ_{i_k} не находится в отношениях «родитель — потомок» с любой другой вершиной τ_{i_m} того же подмножества: $\tau_{i_k} \lessgtr \tau_{i_m}$, где $k \neq m$; $\lessgtr$ — знак несравнимости, т. е. неподчинённости по корневому дереву иерархического классификатора (если объект помечен рубрикой родителя, то он содержит тематику и всех подчинённых рубрик-потомков, так что указывать их в его тематическом индексе нет необходимости);

б) в подмножестве $\{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_L}\}$ не содержится полного набора сыновей ни одной из вершин корневого дерева иерархического классификатора (если тематика объекта содержит полный набор сыновей какой-либо рубрики, то в тематический индекс объекта вместо этого набора сыновей необходимо и достаточно внести родительскую рубрику).

На рис. 4 наборы рубрик $\mathcal{T}_1^{\mathsf{M}} = \{\tau_2, \tau_{12}, \tau_{19}\}$ и $\mathcal{T}_2^{\mathsf{M}} = \{\tau_7, \tau_9, \tau_{13}, \tau_{15}, \tau_{16}\}$ являются мультирубриками, наборы рубрик $\mathcal{T}_1 = \{\tau_6, \tau_{14}\}$ и $\mathcal{T}_2 = \{\tau_{13}, \tau_{17}, \tau_{18}\}$ требованиям для мультирубрики не удовлетворяют, поскольку τ_6 и τ_{14} связаны отношением «родитель — потомок», а τ_{17} и τ_{18} образуют полный набор сыновей рубрики τ_{12}.

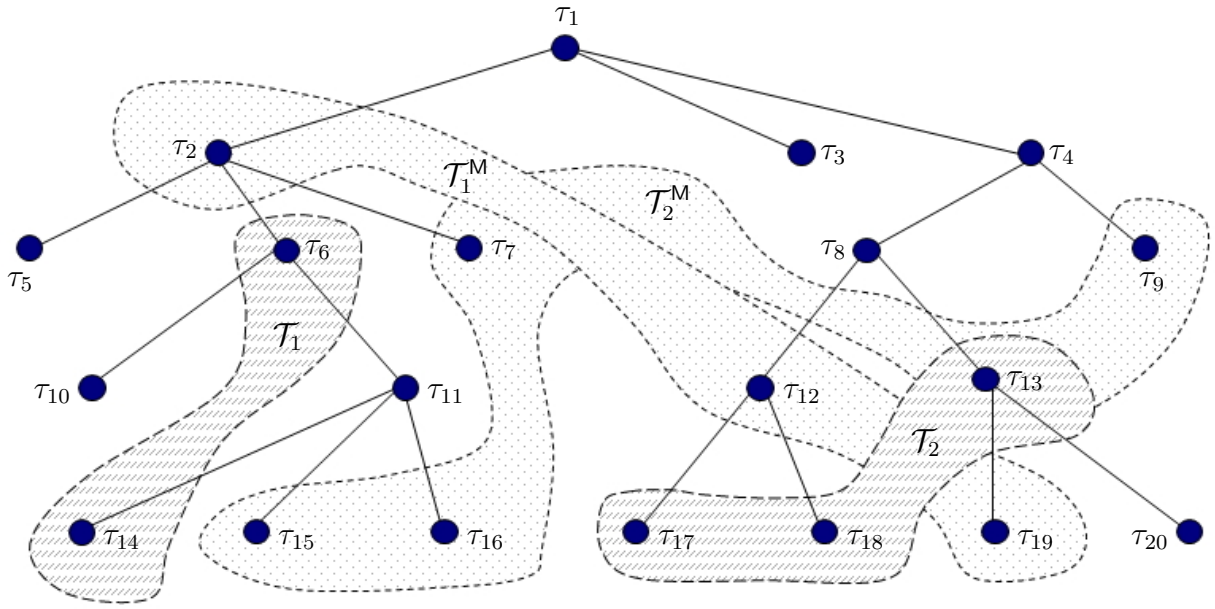


Рис. 4. Примеры наборов рубрик, являющихся мультирубриками ($\mathcal{T}_1^{\mathsf{M}}, \mathcal{T}_2^{\mathsf{M}}$) и не являющихся мультирубриками ($\mathcal{T}_1, \mathcal{T}_2$)

Множество всех мультирубрик на корневом дереве классификатора будем обозначать T^{M} ($\mathcal{T}_i^{\mathsf{M}} \in T^{\mathsf{M}}$).

Отметим, что по определению 1 мультирубриками являются также набор из одной рубрики (вершины классификатора) и пустой набор рубрик-вершин $\varnothing \in T^{\mathsf{M}}$.

Поскольку рубрики τ_k, входящие в различные мультирубрики, могут находиться в отношениях подчинённости («родитель — потомок»), то отношения «шире — уже»,

т. е. доминирования одной мультирубрики над другой, не могут адекватно воспроизводиться отношением теоретико-множественного включения.

Определение 2. Мультирубрика $\mathcal{T}_i^{\mathsf{M}} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$ доминирует над мультирубрикой $\mathcal{T}_j^{\mathsf{M}} = \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\}$ (шире или равна по тематике; для обозначения доминирования мультирубрик будем использовать знак $\leqslant_{\mathsf{M}}$) в том и только в том случае, когда для любого $m = 1, \ldots, J$ существует $n = 1, \ldots, I$, такое, что $\tau_{j_m} \leqslant \tau_{i_n}$ (вершина $\tau_{j_m} \in \mathcal{T}_j^{\mathsf{M}}$ подчинена по корневому дереву иерархического классификатора вершине $\tau_{i_n} \in \mathcal{T}_i^{\mathsf{M}}$ или τ_{j_m} и τ_{i_n} совпадают):

$$\mathcal{T}_j^{\mathsf{M}} \leqslant_{\mathsf{M}} \mathcal{T}_i^{\mathsf{M}} \quad \Leftrightarrow \quad \forall \tau_{j_m} \in \mathcal{T}_j^{\mathsf{M}}\, \exists \tau_{i_n} \in \mathcal{T}_i^{\mathsf{M}}\, (\tau_{j_m} \leqslant \tau_{i_n}).$$

Заметим, что если ни $\mathcal{T}_i^{\mathsf{M}}$ не доминирует над $\mathcal{T}_j^{\mathsf{M}}$, ни $\mathcal{T}_j^{\mathsf{M}}$ не доминирует над $\mathcal{T}_i^{\mathsf{M}}$, то мультирубрики $\mathcal{T}_i^{\mathsf{M}}$ и $\mathcal{T}_j^{\mathsf{M}}$ являются *несравнимыми*; для обозначения этого будем использовать знак $\leqslant_{\mathsf{M}}\geqslant$. При этом часть рубрик-вершин $\tau_{i_n} \in \mathcal{T}_i^{\mathsf{M}}$ и $\tau_{j_m} \in \mathcal{T}_j^{\mathsf{M}}$ могут совпадать или находиться в отношении «родитель — потомок».

На рис. 5 приведены примеры доминирования и несравнимости мультирубрик.

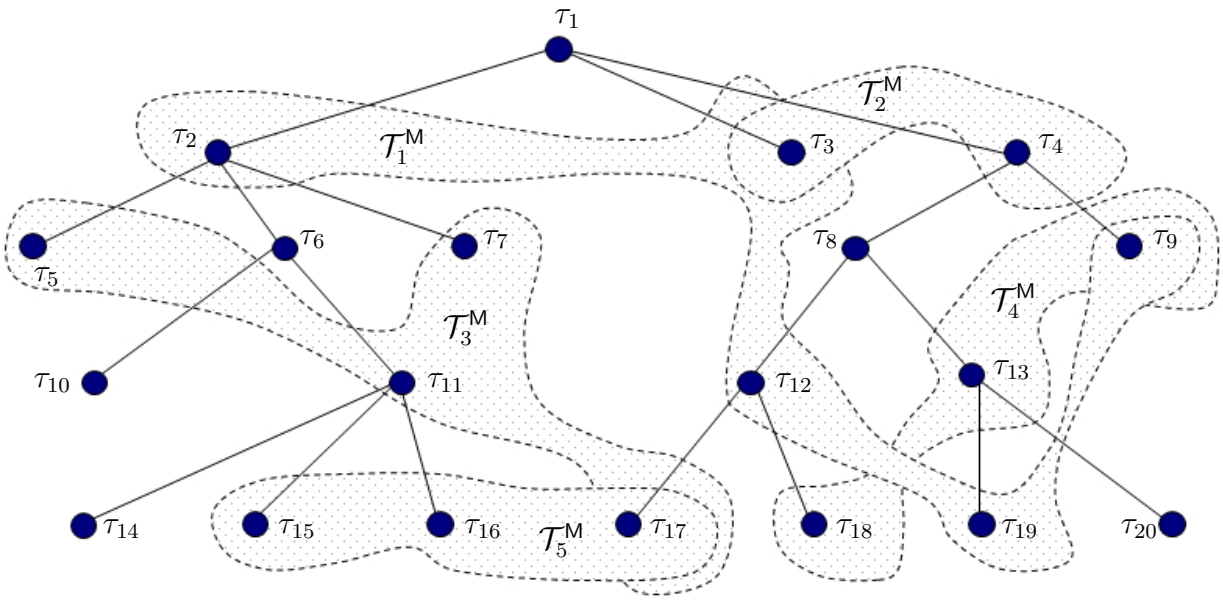


Рис. 5. Примеры доминирования и несравнимости мультирубрик: $\mathcal{T}_5^{\mathsf{M}} \leqslant_{\mathsf{M}} \mathcal{T}_3^{\mathsf{M}} \leqslant_{\mathsf{M}} \mathcal{T}_1^{\mathsf{M}}$, $\mathcal{T}_4^{\mathsf{M}} \leqslant_{\mathsf{M}} \mathcal{T}_2^{\mathsf{M}}$, $\mathcal{T}_1^{\mathsf{M}} \leqslant_{\mathsf{M}}\geqslant \mathcal{T}_2^{\mathsf{M}}$, $\mathcal{T}_2^{\mathsf{M}} \leqslant_{\mathsf{M}}\geqslant \mathcal{T}_5^{\mathsf{M}}$, $\mathcal{T}_3^{\mathsf{M}} \leqslant_{\mathsf{M}}\geqslant \mathcal{T}_2^{\mathsf{M}}$

Таким образом, определение 2 устанавливает на множестве мультирубрик T^{M} отношение частичного порядка.

Для построения решётки мультирубрик необходимо определить операции получения точных границ (наименьшей верхней и наибольшей нижней) для любых пар мультирубрик. Как и в случае с отношением доминирования, операции теоретико-множественного объединения и пересечения в отношении наборов рубрик, составляющих мультирубрики, не подходят.

Определение 3. Иерархическим сжатием $\sqcup_{\mathsf{H}}$ множества элементов $\{\tau_{k_1}, \tau_{k_2}, \ldots, \tau_{k_L}\}$ $(L < K)$, являющихся вершинами корневого дерева, задающего частичный порядок на множестве рубрик иерархического классификатора $T_{\mathsf{H}} = \{\tau_1, \tau_2, \ldots, \tau_K\}$, будем называть итеративную операцию замены вершинами-родителями любых подмножеств элементов, являющихся в множестве $\{\tau_{k_1}, \tau_{k_2}, \ldots, \tau_{k_L}\}$ полными наборами сыновей соответствующих вершин-родителей.

К примеру, иерархическое сжатие набора вершин $\mathcal{T}_2 = \{\tau_{13}, \tau_{17}, \tau_{18}\}$ на рис. 4 даёт набор из одной вершины-рубрики $\{\tau_8\}$:

$$\sqcup_{\mathsf{H}}(\mathcal{T}_2) = \sqcup_{\mathsf{H}}\{\tau_{13}, \tau_{17}, \tau_{18}\} = \sqcup_{\mathsf{H}}\{\tau_{13}, \tau_{12}\} = \{\tau_8\}.$$

Отметим, что иерархическое сжатие по набору рубрик какой-либо мультирубрики является в соответствии с определением 1 той же мультирубрикой:

$$\sqcup_{\mathsf{H}}(\mathcal{T}_i^{\mathsf{M}}) = \sqcup_{\mathsf{H}}\{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\} = \mathcal{T}_i^{\mathsf{M}}.$$

Введём понятия объединения и пересечения мультирубрик.

Определение 4. Объединением $\cup_{\mathsf{M}}$ мультирубрик $\mathcal{T}_i^{\mathsf{M}} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$ и $\mathcal{T}_j^{\mathsf{M}} = \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\}$ называется операция формирования множества вершин иерархического рубрикатора $\mathcal{T}^{\mathsf{M}\cup} = \mathcal{T}_i^{\mathsf{M}} \cup_{\mathsf{M}} \mathcal{T}_j^{\mathsf{M}}$ на основе следующего алгоритма:

а) формируется теоретико-множественное объединение $\mathcal{T}^{\cup}$ множеств вершин, составляющих мультирубрики:

$$\mathcal{T}^{\cup} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\} \cup \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\};$$

б) формируется набор вершин $\mathcal{T}^{\cup'}$ путем исключения из набора $\mathcal{T}^{\cup}$ тех вершин τ_k, для которых хотя бы одна вершина из того же набора $\mathcal{T}^{\cup}$ является предком:

$$(\tau_k \in \mathcal{T}^{\cup} \wedge \tau_k \notin \mathcal{T}^{\cup'}) \quad \Leftrightarrow \quad \exists \tau_m \in \mathcal{T}^{\cup}\,(\tau_m < \tau_k);$$

в) формируется итоговый набор вершин путём иерархического сжатия набора вершин $\mathcal{T}^{\cup'}$:

$$\mathcal{T}^{\mathsf{M}\cup} = \sqcup_{\mathsf{H}}(\mathcal{T}^{\cup'}).$$

Определение 5. Пересечением $\cap_{\mathsf{M}}$ мультирубрик $\mathcal{T}_i^{\mathsf{M}} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$ и $\mathcal{T}_j^{\mathsf{M}} = \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\}$ называется операция формирования множества вершин иерархического классификатора $\mathcal{T}^{\mathsf{M}\cap} = \mathcal{T}_i^{\mathsf{M}} \cap_{\mathsf{M}} \mathcal{T}_j^{\mathsf{M}}$ на основе следующего алгоритма:

а) из множества вершин мультирубрики $\mathcal{T}_i^{\mathsf{M}}$ формируется множество вершин $\mathcal{T}_i^{\mathsf{M}'}$, для которых в наборе вершин мультирубрики $\mathcal{T}_j^{\mathsf{M}}$ найдётся совпадающая вершина или вершина-предок:

$$(\tau_k \in \mathcal{T}_i^{\mathsf{M}} \wedge \tau_k \in \mathcal{T}_i^{\mathsf{M}'}) \quad \Leftrightarrow \quad \exists \tau_m \in \mathcal{T}_j^{\mathsf{M}}\,(\tau_k \leqslant \tau_m);$$

б) из множества вершин мультирубрики $\mathcal{T}_j^{\mathsf{M}}$ формируется множество вершин $\mathcal{T}_j^{\mathsf{M}'}$, для которых в наборе вершин мультирубрики $\mathcal{T}_i^{\mathsf{M}}$ найдётся совпадающая вершина или вершина-предок:

$$(\tau_k \in \mathcal{T}_j^{\mathsf{M}} \wedge \tau_k \in \mathcal{T}_j^{\mathsf{M}'}) \quad \Leftrightarrow \quad \exists \tau_m \in \mathcal{T}_i^{\mathsf{M}}\,(\tau_k \leqslant \tau_m);$$

в) осуществляется теоретико-множественное объединение множеств $\mathcal{T}_i^{\mathsf{M}'}$ и $\mathcal{T}_j^{\mathsf{M}'}$:

$$\mathcal{T}^{\mathsf{M}\cap} = \mathcal{T}_i^{\mathsf{M}'} \cup_{\mathsf{M}} \mathcal{T}_j^{\mathsf{M}'}.$$

Отметим, что по алгоритму определения 5, если мультирубрики $\mathcal{T}_i^{\mathsf{M}}$ и $\mathcal{T}_j^{\mathsf{M}}$ содержат только несравнимые вершины, то результатом их пересечения будет пустое множество.

Нетрудно доказать [6], что множества $\mathcal{T}^{\mathsf{M}\cup} = \mathcal{T}_i^{\mathsf{M}} \cup_{\mathsf{M}} \mathcal{T}_j^{\mathsf{M}}$ и $\mathcal{T}^{\mathsf{M}\cap} = \mathcal{T}_i^{\mathsf{M}} \cap_{\mathsf{M}} \cap_{\mathsf{M}} \mathcal{T}_j^{\mathsf{M}}$ являются а) мультирубриками и б) наименьшей верхней границей и наибольшей нижней границей для мультирубрик $\mathcal{T}_i^{\mathsf{M}}$ и $\mathcal{T}_j^{\mathsf{M}}$ соответственно.

На рис. 6 приведён пример объединения и пересечения мультирубрик, иллюстрирующий, насколько данные операции отличаются от обычных операций объединения и пересечения множеств.

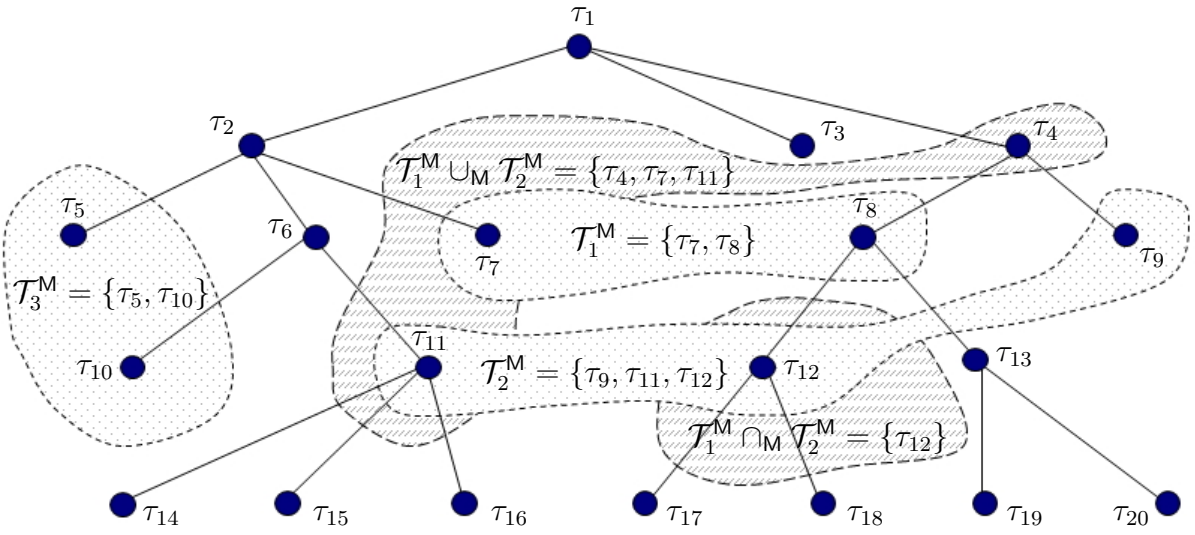


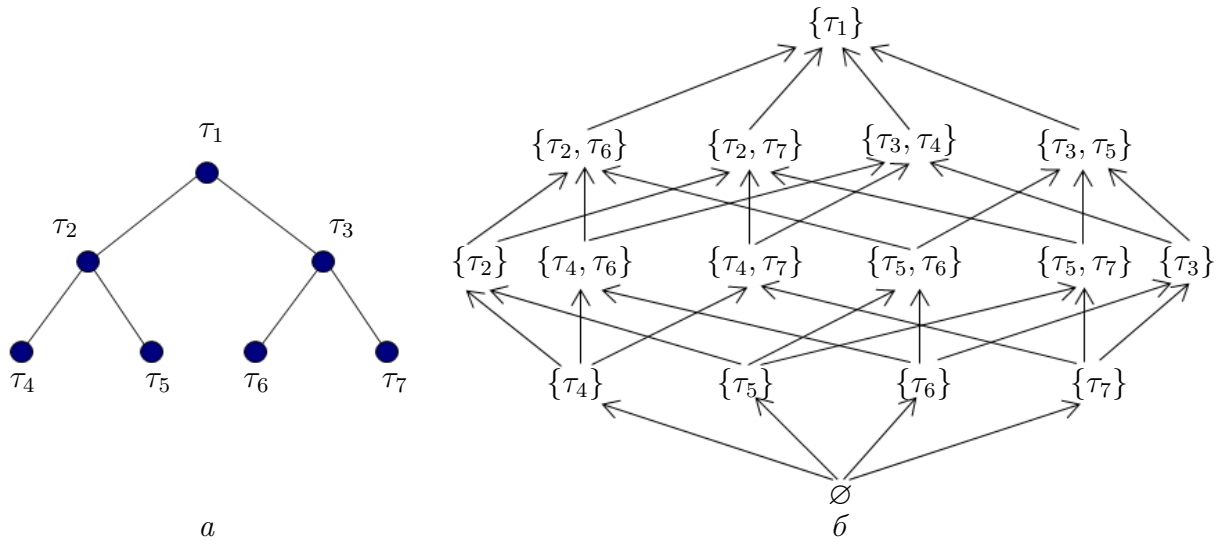
Рис. 6. Пример объединения и пересечения мультирубрик: $\mathcal{T}_1^{\mathsf{M}} \cup_{\mathsf{M}} \mathcal{T}_2^{\mathsf{M}} = \{\tau_7, \tau_8\} \cup_{\mathsf{M}} \cup_{\mathsf{M}} \{\tau_9, \tau_{11}, \tau_{12}\} = \{\tau_4, \tau_7, \tau_{11}\}$; $\mathcal{T}_1^{\mathsf{M}} \cap_{\mathsf{M}} \mathcal{T}_2^{\mathsf{M}} = \{\tau_7, \tau_8\} \cap_{\mathsf{M}} \{\tau_9, \tau_{11}, \tau_{12}\} = \{\tau_{12}\}$; $\mathcal{T}_1^{\mathsf{M}} \cap_{\mathsf{M}} \mathcal{T}_3^{\mathsf{M}} = \varnothing$; $\mathcal{T}_2^{\mathsf{M}} \cap_{\mathsf{M}} \mathcal{T}_3^{\mathsf{M}} = \varnothing$

Заметим, что объединение и пересечение мультирубрик, одна из которых доминирует над другой, дает доминирующую или доминируемую мультирубрику соответственно:

$$\mathcal{T}_j^{\mathsf{M}} \leqslant_{\mathsf{M}} \mathcal{T}_i^{\mathsf{M}} \Rightarrow \mathcal{T}_j^{\mathsf{M}} \cup_{\mathsf{M}} \mathcal{T}_i^{\mathsf{M}} = \mathcal{T}_i^{\mathsf{M}}, \quad \mathcal{T}_j^{\mathsf{M}} \cap_{\mathsf{M}} \mathcal{T}_i^{\mathsf{M}} = \mathcal{T}_j^{\mathsf{M}}.$$

В результате имеем решётку мультирубрик $\Lambda_{\mathsf{TH}}(T^{\mathsf{M}}, \leqslant_{\mathsf{M}}, \cup_{\mathsf{M}}, \cap_{\mathsf{M}})$.

На рис. 7 для простейшего иерархического рубрикатора приведена диаграмма Хассе решётки мультирубрик.



а *б*

Рис. 7. Иерархический рубрикатор (*а*); диаграмма Хассе решётки мультирубрик для него (*б*)

Используя линейную решётку уровней безопасности $\Lambda_{\mathsf{L}}(L, <, \circ, \otimes)$ и решётку мультирубрик $\Lambda_{\mathsf{TH}}(T^{\mathsf{M}}, \leqslant_{\mathsf{M}}, \cup_{\mathsf{M}}, \cap_{\mathsf{M}})$, можно построить модель безопасности, основанную

на объединении модели Белла — ЛаПадулы и тематико-иерархического разграничения доступа.

3. MLTHS-система

Будем строить MLTHS-систему на базе аппарата *субъектно-объектных моделей конечных состояний* [1, 3, 7], основные положения которых сводятся к следующему:

1. В контексте безопасности компьютерная система представляется совокупностью *объектов* доступа $o \in O$ и управляемых пользователями *субъектов* доступа $s \in S$.

2. Объекты доступа $o \in O$ рассматриваются как слова (совокупность слов, запись), характеризующие относительно некоторого языка **Я** состояния логических (файлы, каталоги, таблицы и т. д.) или физических элементов (порты, принтеры, приводы и т. д.).

3. Субъекты доступа $s \in S$ рассматриваются как активизированные состояния специальных объектов (*объектов-источников*), описывающих относительно некоторого языка *преобразования информации* (отображение одного слова в другое), при котором инициализированным, т. е. действующим преобразованиям выделены определённые вычислительные ресурсы (*домен преобразования*) и передано управление компьютерной системой. В некоторых источниках вместо понятия «домен субъекта доступа» используют понятие «функционально или параметрически ассоциированных с субъектом объектов доступа».

4. Субъекты осуществляют *доступы* к объектам (рис. 8), в результате которых возникают *информационные потоки*, заключающиеся в изменении слов, характеризующих или объект доступа (доступ *на запись* в объект — `w`), или *домен* субъекта доступа (доступ *на чтение* из объекта — `r`), или инициализирующих активизацию объектов-источников с выделением домена и передачей управления (доступ *на выполнение* объекта-источника — `e`).

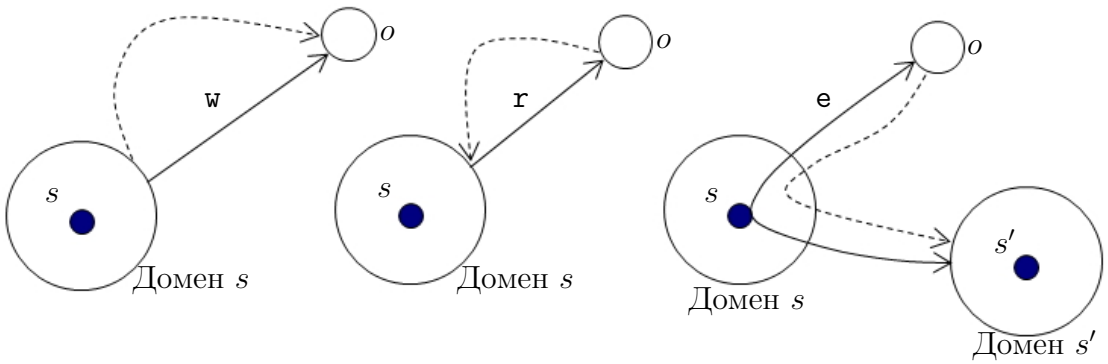


Рис. 8. Доступы на запись (`w`), чтение (`r`), выполнение (`e`) и соответствующие им информационные потоки (штриховые линии со стрелками)

5. В компьютерной системе действует дискретное время, в каждый момент которого t_k состояние системы V_k характеризуется определённой декомпозицией на множество субъектов S, осуществляющих доступы на множестве объектов O, в результате чего формируются информационные потоки, переводящие в момент времени t_{k+1} систему в новое состояние V_{k+1}.

6. Помимо субъектов доступа, управляемых пользователями, в системе изначально (в том числе в момент времени t_0) присутствуют *системные субъекты*, используя сервис которых, пользователи, начиная работу в системе, инициализируют свои первичные субъекты.

7. *Информационные потоки*, вызываемые доступами субъектов к объектам, по правилам (критериям) политики безопасности разделяются на неопасные (*допустимые*) и опасные (*недопустимые*), результатом которых может быть нарушение конфиденциальности и/или целостности и/или правомерной доступности объектов (информации).

8. В подмножестве системных субъектов действует *монитор безопасности*, санкционирующий по правилам (критериям) политики безопасности запросы субъектов на доступ к объектам.

9. Проблема безопасности, которую должна разрешать модель безопасности, заключается в формальном доказательстве того факта, что при условии отсутствия опасных (недопустимых) информационных потоков в начальном состоянии V_0 и санкционировании монитором безопасности только тех запросов на доступ, которые удовлетворяют правилам (критериям) безопасности, при переходе в состояние V_k не возникло недопустимых информационных потоков.

Основные положения MLTHS-системы сводятся к следующему.

Положение 1. Тематика информации, обрабатываемой в компьютерной системе, отображается иерархическим тематическим классификатором, представляющим собой конечное множество тематических рубрик $T_{\mathsf{H}} = \{\tau_1, \tau_2, \ldots, \tau_K\}$, на котором установлен частичный порядок, задаваемый корневым деревом, и множество мультирубрик которого представляет решётку $\Lambda_{\mathsf{TH}}(T^{\mathsf{M}}, \leqslant_{\mathsf{M}}, \cup_{\mathsf{M}}, \cap_{\mathsf{M}})$.

Положение 2. Конфиденциальность (ценность) информации измеряется в порядковой шкале L, конечное множество уровней которой является линейной решёткой уровней безопасности $\Lambda_{\mathsf{L}}(L, <, \circ, \otimes)$.

Положение 3. Множество сущностей системы (субъектов S и объектов доступа O) отображается в произведение линейной решётки уровней безопасности $\Lambda_{\mathsf{L}}(L, <, \circ, \otimes)$ и решётки мультирубрик $\Lambda_{\mathsf{TH}}(T^{\mathsf{M}}, \leqslant_{\mathsf{M}}, \cup_{\mathsf{M}}, \cap_{\mathsf{M}})$.

На рис. 9 представлена диаграмма Хассе произведения простейшей решётки из двух уровней безопасности ($l_1 > l_2$) и решётки мультирубрик (рис. 7, *б*) для простейшего иерархического тематического классификатора.

Произведение решёток $\Lambda_{\mathsf{L}}(L, <, \circ, \otimes)$ и $\Lambda_{\mathsf{TH}}(T^{\mathsf{M}}, \leqslant_{\mathsf{M}}, \cup_{\mathsf{M}}, \cap_{\mathsf{M}})$ будем называть *мандатной тематико-иерархической решёткой*.

В результате каждый экземпляр сущности $x \in (S \cup O)$ характеризуется меткой безопасности $\mathcal{F}_{\mathsf{LTH}}(x)$, состоящей из уровня безопасности $l \in L$ и мультирубрики $\mathcal{T}^{\mathsf{M}} \in T^{\mathsf{M}}$: $\mathcal{F}_{\mathsf{LTH}}(x) = \{l_x, \mathcal{T}_x^{\mathsf{M}}\}$.

Заметим, что из $\mathcal{F}_{\mathsf{LTH}}(x_1) \leqslant \mathcal{F}_{\mathsf{LTH}}(x_2)$ следует $(l_{x_1} \leqslant l_{x_2}) \wedge (\mathcal{T}_{x_1}^{\mathsf{M}} \leqslant_{\mathsf{M}} \mathcal{T}_{x_1}^{\mathsf{M}})$. В противном случае $\mathcal{F}_{\mathsf{LTH}}(x_1)$ и $\mathcal{F}_{\mathsf{LTH}}(x_2)$ *несравнимы* (рис. 9). Таким образом, на множестве меток безопасности $\mathcal{F}_{\mathsf{LTH}}(x)$ имеется частичный порядок. Далее, если $\mathcal{F}_{\mathsf{LTH}}(x_1) \leqslant \mathcal{F}_{\mathsf{LTH}}(x_2)$, то будем говорить, что метка $\mathcal{F}_{\mathsf{LTH}}(x_2)$ выше (или равна) метки $\mathcal{F}_{\mathsf{LTH}}(x_1)$.

Положение 4. Доверительно-тематические *полномочия пользователей* $\mathcal{F}_{\mathsf{LTH}}(s) = \{l_s, \mathcal{T}_s^{\mathsf{M}}\}$ задаются внешним по отношению к компьютерной системе фактором посредством присвоения их регистрационным записям меток безопасности. Таким образом, вопросы безопасности, связанные с изменением уровней допуска и/или тематических полномочий пользователей, моделью MLTHS-системы не охватываются.

Положение 5. Все системные субъекты, кроме монитора безопасности, имеют метку безопасности $(l_{\min}, \varnothing)$. Монитор безопасности имеет метку $(l_{\max}, \{\tau_1\})$.

Положение 6. Пользователи, начиная работу в системе, посредством сервиса системных субъектов инициализируют свои первичные субъекты, которым монитор безопасности присваивает метки безопасности их регистрационных записей.

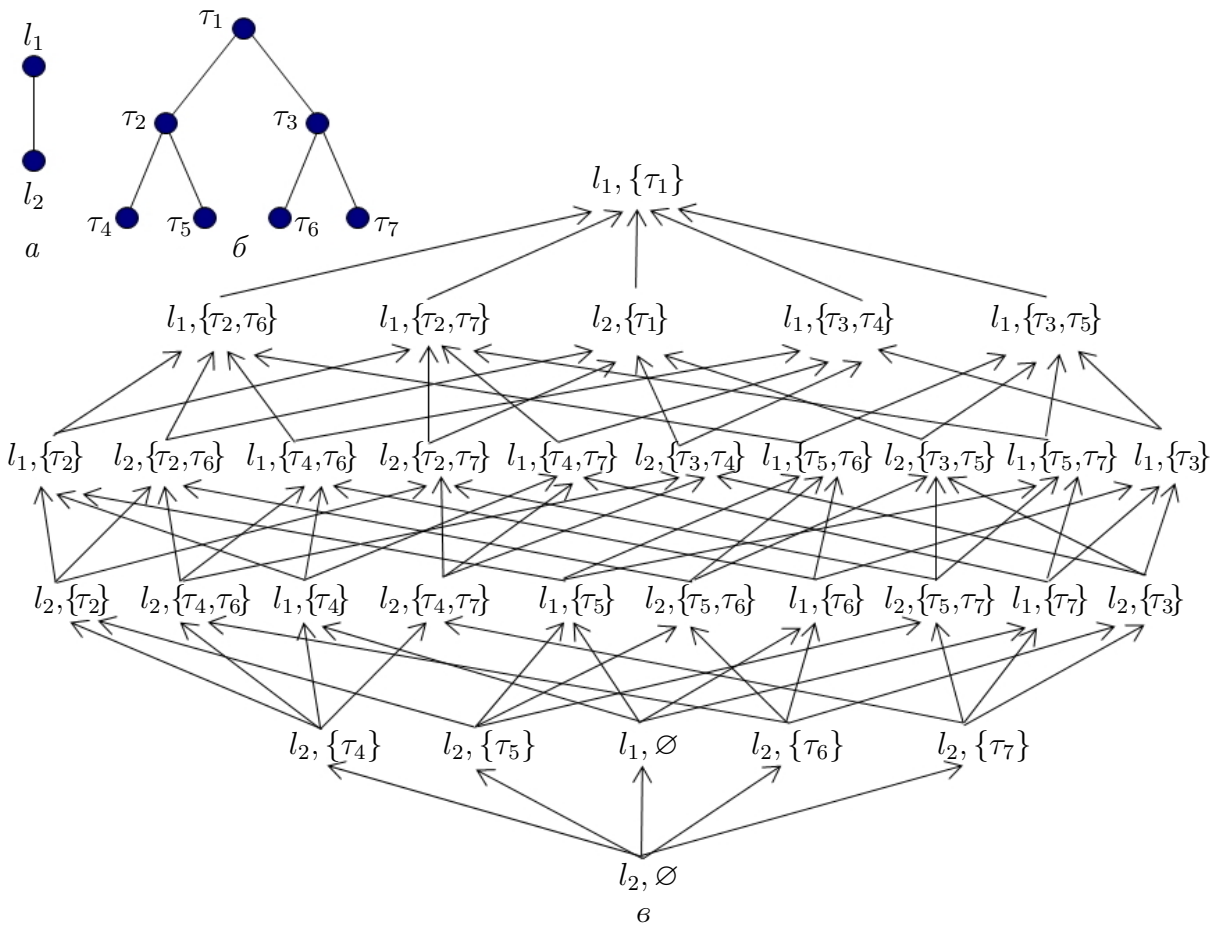


Рис. 9. Решётка уровней безопасности ($а$); иерархический тематический классификатор ($б$); диаграмма Хассе произведения решётки уровней безопасности и решётки мультирубрик ($в$)

Определение 6 (критерий безопасности). MLTHS-система безопасна тогда и только тогда, когда в ней отсутствуют информационные потоки следующих видов: от сущностей с более высокой меткой безопасности к сущностям с более низкой меткой безопасности; между несравнимыми по меткам безопасности сущностями.

Положение 7. Переходы системы из одного состояния V_k в другое состояние V_{k+1}, обусловленные осуществлением доступов существующих субъектов к существующим объектам, санкционируются монитором безопасности на основе следующих правил, вытекающих из критерия, задаваемого определением 6:

П р а в и л о 1. Доступ субъекта s к объекту o, вызывающий поток по чтению (`r`), неопасен и может быть разрешён монитором безопасности тогда и только тогда, когда метка безопасности субъекта доминирует над меткой безопасности объекта:

$$\mathcal{F}_{\mathsf{LTH}}[s] \geqslant \mathcal{F}_{\mathsf{LTH}}[o].$$

П р а в и л о 2. Доступ субъекта s к объекту o, вызывающий поток по записи (`w`), неопасен и может быть разрешён монитором безопасности тогда и только тогда, когда метка безопасности объекта доминирует над меткой безопасности субъекта:

$$\mathcal{F}_{\mathsf{LTH}}[o] \geqslant \mathcal{F}_{\mathsf{LTH}}[s].$$

Положение 8. Переходы системы из одного состояния V_k в другое состояние V_{k+1}, связанные с созданием новых объектов, санкционируются монитором безопасности на основе следующего правила:

П р а в и л о 3. Создание субъектом s нового объекта o', в том числе за счёт чтения из другого объекта o, вызывает неопасный поток и может быть разрешено монитором безопасности тогда и только тогда, когда метка безопасности субъекта доминирует над меткой объекта o, при этом монитор безопасности присваивает новому объекту o' мультирубрику, доминирующую над мультирубрикой субъекта:

$$\mathcal{F}_{\mathsf{LTH}}[o] \leqslant \mathcal{F}_{\mathsf{LTH}}[s] \leqslant \mathcal{F}_{\mathsf{LTH}}[o'].$$

Присвоение новому объекту метки безопасности, строго большей, чем метка безопасности субъекта ($\mathcal{F}_{\mathsf{LTH}}[s] < \mathcal{F}_{\mathsf{LTH}}[o']$), осуществляется монитором безопасности по специальному запросу к субъекту. В противном случае новому объекту присваивается метка безопасности субъекта ($\mathcal{F}_{\mathsf{LTH}}[s] \equiv \mathcal{F}_{\mathsf{LTH}}[o']$).

С учётом положений 4 и 6, при инициализации новых субъектов действует следующее правило:

П р а в и л о 4. Инициализация субъектом s нового субъекта s' посредством воздействия на объект-источник o (доступ $\mathtt{e}$) вызывает неопасный поток и может быть разрешена монитором безопасности тогда и только тогда, когда метка безопасности субъекта доминирует над меткой безопасности объекта-источника, при этом монитор безопасности присваивает новому субъекту метку безопасности, тождественную метке безопасности инициализирующего субъекта:

$$\mathcal{F}_{\mathsf{LTH}}[o] \leqslant \mathcal{F}_{\mathsf{LTH}}[s] \equiv \mathcal{F}_{\mathsf{LTH}}[s'].$$

Положение 9. Переходы системы из одного состояния V_k в другое состояние V_{k+1}, связанные с одновременными множественными доступами с учётом транзитивности информационных потоков и отношений доминирования меток безопасности, осуществляются на основе следующего правила:

П р а в и л о 5. Одновременный доступ субъекта s к объектам $o_1, o_2, \ldots$ или субъектов $s_1, s_2, \ldots$ к объекту o может быть разрешён (неопасен) тогда и только тогда, когда каждый одиночный доступ из запрашиваемой совокупности доступов удовлетворяет правилам 1–4.

В технологическом отношении реализация правила 5 может осуществляться на основе операций взятия наименьшей верхней границы или наибольшей нижней границы меток безопасности объектов $o_1, o_2, \ldots$ или субъектов $s_1, s_2, \ldots$ (рис. 10).

Условия доступа на чтение ($\mathtt{r}$) субъекта s одновременно к нескольким объектам $o_1, o_2, \ldots$:

$$(l_s \geqslant \max[l_{o_1}, l_{o_2}, \ldots]) \wedge (\mathcal{T}_s^{\mathsf{M}} \geqslant_{\mathsf{M}} (\mathcal{T}_{o_1}^{\mathsf{M}} \cup_{\mathsf{M}} \mathcal{T}_{o_2}^{\mathsf{M}} \cup_{\mathsf{M}} \ldots)).$$

Условия доступа на запись ($\mathtt{w}$) субъекта s одновременно к нескольким объектам $o_1, o_2, \ldots$:

$$(l_s \leqslant \min[l_{o_1}, l_{o_2}, \ldots]) \wedge (\mathcal{T}_s^{\mathsf{M}} \leqslant_{\mathsf{M}} (\mathcal{T}_{o_1}^{\mathsf{M}} \cap_{\mathsf{M}} \mathcal{T}_{o_2}^{\mathsf{M}} \cap_{\mathsf{M}} \ldots)).$$

Условия доступа на чтение ($\mathtt{r}$) одновременно нескольких субъектов $s_1, s_2, \ldots$ к одному объекту o:

$$(l_o \leqslant \min[l_{s_1}, l_{s_2}, \ldots]) \wedge (\mathcal{T}_o^{\mathsf{M}} \leqslant_{\mathsf{M}} (\mathcal{T}_{s_1}^{\mathsf{M}} \cap_{\mathsf{M}} \mathcal{T}_{s_2}^{\mathsf{M}} \cap_{\mathsf{M}} \ldots)).$$

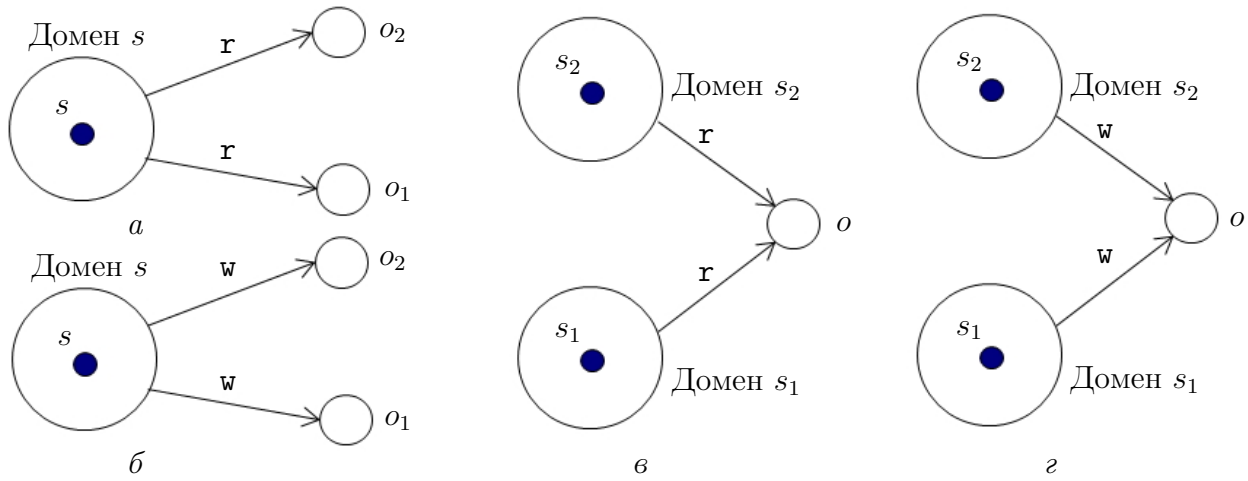


Рис. 10. Множественные доступы: a — одного субъекта по чтению одновременно к двум объектам; $б$ — одного субъекта по записи одновременно к двум объектам; $в$ — по чтению к одному объекту одновременно двух субъектов; $г$ — по записи к одному объекту одновременно двух субъектов

Условия доступа на запись (w) одновременно нескольких субъектов $s_1, s_2, \ldots$ к одному объекту o:

$$(l_o \geqslant \max[l_{s_1}, l_{s_2}, \ldots]) \wedge (\mathcal{T}_o^{\mathsf{M}} \geqslant_{\mathsf{M}} (\mathcal{T}_{s_1}^{\mathsf{M}} \cup_{\mathsf{M}} \mathcal{T}_{s_2}^{\mathsf{M}} \cup_{\mathsf{M}} \ldots)).$$

Справедливо следующее утверждение:

Утверждение 1. В MLTHS-системе реализуется множество только таких потоков, которые удовлетворяют критерию безопасности по определению 6.

Доказательство. В соответствии с положениями субъектно-объектных моделей конечных состояний в начальном состоянии V_0 потоки от сущностей с более высокой (доминирующей) меткой безопасности к сущностям с более низкой меткой безопасности, а также потоки между несравнимыми по меткам безопасности сущностями отсутствуют. Необходимо доказать, что при последовательном переходе системы в состояние V_k на основе доступов, которые санкционируются по правилам 1–5, таких потоков также не появится.

Утверждение очевидно для переходов, реализуемых на основе одиночных доступов, которые санкционируются по правилам 1–4, в том числе и для потоков, связанных с созданием новых объектов и инициализацией новых субъектов доступа.

В случае переходов, вызываемых одновременными множественными доступами только по чтению или только по записи (одним субъектом одновременно к множеству объектов или множеством субъектов одновременно к одному объекту) также очевидно, что опасные потоки не могут реализоваться в соответствии с правилом 5.

Рассмотрим доступы одного субъекта одновременно к части объектов по чтению, а к части объектов по записи и, аналогично, доступы к одному объекту частью субъектов по чтению, а частью субъектов по записи. По свойству транзитивности такие доступы могут реализовывать информационные потоки от одного объекта к другому объекту или от одного субъекта к другому субъекту (рис. 11).

По условиям утверждения 1 при санкционировании доступа, вызывающего поток $o_1 \to o_2$, имеем

$$(\mathcal{F}_{\mathsf{LTH}}[s] \geqslant \mathcal{F}_{\mathsf{LTH}}[o_1]) \wedge (\mathcal{F}_{\mathsf{LTH}}[o_2] \geqslant \mathcal{F}_{\mathsf{LTH}}[s]).$$

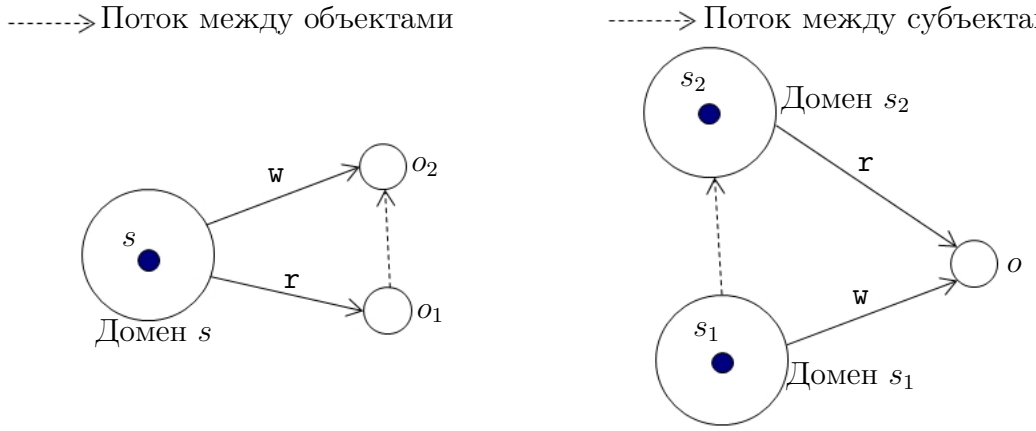


Рис. 11. Множественные доступы, вызывающие по свойству транзитивности потоки между объектами и между субъектами

Отсюда следует, что

$$\mathcal{F}_{\mathsf{LTH}}[o_2] \geqslant \mathcal{F}_{\mathsf{LTH}}[o_1].$$

Таким образом, осуществляется неопасный поток «снизу вверх» между сравнимыми по меткам безопасности сущностями.

Аналогично по условиям утверждения 1 при санкционировании потока $s_1 \to s_2$ имеем

$$(\mathcal{F}_{\mathsf{LTH}}[s_1] \leqslant \mathcal{F}_{\mathsf{LTH}}[o]) \wedge (\mathcal{F}_{\mathsf{LTH}}[s_2] \geqslant \mathcal{F}_{\mathsf{LTH}}[o]).$$

Отсюда следует, что

$$\mathcal{F}_{\mathsf{LTH}}[s_2] \geqslant \mathcal{F}_{\mathsf{LTH}}[s_1].$$

Таким образом, и в этом случае осуществляется неопасный поток «снизу вверх».

Нетрудно видеть, что любые другие множественные потоки являются комбинацией двух рассмотренных потоков $o_1 \to o_2$ и $s_1 \to s_2$, из чего по свойству транзитивности вытекает наличие в системе только неопасных потоков, т. е. потоков, удовлетворяющих критерию безопасности по определению 6. ■

Заключение

MLTHS-система, как и MLS-система с неиерархическими рубриками-категориями, реализуя одновременно доверительно-мандатный и тематический принципы, позволяет гораздо детальнее обеспечить разграничение доступа к информации. В классической модели Белла — ЛаПадулы для детализации доступа приходится вводить матрицу доступа, что соответственно привносит проблемы безопасности, присущие дискреционным моделям, в частности, проблему троянских программ в рамках разграничения доступа к объектам одного уровня безопасности.

При этом, в отличие от простейшего дескрипторно-тематического подхода в MLS-системе, тематический доступ в MLTHS-системе основывается на иерархических классификаторах, повсеместно применяемых в организации информационно-поисковых хранилищ документов. В результате имеется возможность соединить технологии текстового поиска в документальных хранилищах и технологии разграничения доступа, создавая на этой основе защищённые документально-поисковые системы без ограничения их функциональности.

ЛИТЕРАТУРА

1. *Грушо А. А., Применко Е. А., Тимонина Е. Е.* Теоретические основы компьютерной безопасности. М.: Издательский центр «Академия», 2009. 272 с.
2. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. М.: Горячая линия — Телеком, 2011. 320 с.
3. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с.
4. *Bell D. E. and LaPadula L. J.* Secure Computers Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976.
5. *Крюков К. В., Панкова Л. А., Пронина В. А. и др.* Меры семантической близости в онтологии // Пробл. управл. 2010. № 5. С. 2–14.
6. *Гайдамакин Н. А.* Модель тематического разграничения доступа к информации при иерархической структуре классификатора в автоматизированных системах управления // Автоматика и телемеханика. 2003. № 3. С. 177–189.
7. *Щербаков А. Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009. 352 с.

REFERENCES

1. *Grusho A. A., Primenko E. A., and Timonina E. E.* Teoreticheskie osnovy komp'yuternoy bezopasnosti [Theoretical Foundations of Computer Security]. Moscow, Akademiya Publ., 2009. 272 p. (in Russian)
2. *Devyanin P. N.* Modeli bezopasnosti komp'yuternykh sistem. Upravlenie dostupom i informatsionnymi potokami [Models of Computer Systems Security. Control of Access and Information Flows]. Moscow, Goryachaya liniya — Telekom, 2011. 320 p. (in Russian)
3. *Gaydamakin N. A.* Razgranichenie dostupa k informatsii v komp'yuternykh sistemakh [Differentiation of Access to Information in Computer Systems]. Ekaterinburg, USU Publ., 2003. 328 p. (in Russian)
4. *Bell D. E. and LaPadula L. J.* Secure Computers Systems: Unified Exposition and Multics Interpretation. Bedford, Mass., MITRE Corp., 1976.
5. *Kryukov K. V., Pankova L. A., Pronina V. A., et al.* Mery semanticheskoy blizosti v ontologii [Semantic similarity measures in ontology]. Control Science, 2010, no. 5, pp. 2–14. (in Russian)
6. *Gaidamakin N. A.* A model of thematic differentiation of access to information for the hierarchical classifier in automatic control systems. Automaton and Remote Control, 2003, vol. 64, iss. 3, pp. 505–516.
7. *Shcherbakov A. Yu.* Sovremennaya komp'yuternaya bezopasnost'. Teoreticheskie osnovy. Prakticheskie aspekty [Modern Computer Security. Theoretical Basis. Practical Aspects]. Moscow, Knizhnyy mir, 2009. 352 p. (in Russian)