N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 5, Number 297 (2014), 33 – 41

POLYMORPHIC TYPING OF ENTITIES AND A TASK OF CONSTRUCTING MULTI-CRITERIA ACCESS CONTROL MECHANISM

R. G. Bijashev, M. N. Kalimoldaev, O. A. Rog

Institute of information and computing technologies, Almaty, Kazakhstan.
E-mails: mnk@ipic.kz, brg@ipic.kz, olga@ipic.kz

Key words: computer security, mandatory security policy, multi-criteria access control, security domain, type theory, computable functions.

Abstract. Problems of implementation of a formal model of multi-criteria system of access control (MSAC) are considered. This system allow the simultaneous use of a number of security models of mandate type represented in a unified manner, which provides a multi-aspect security access of subjects to objects.

The principle of multi-criteria access control is based on multiple categorization of the entities, implemented in the form of their multiple polymorphic typing. As a result, entity acquires a set of values corresponding to the categories, each of which is mapped to the certain security model.

An algebraic definition of the security model in the form of a pair of the domain security – security policy is given. Security domain corresponds to the category of the MSAC structured on several levels. Security policy is represented as a set of parameterized computable functions for constructing the security domain and setting an access relation on it. A set of such models forms a system of types of the MSAC, serving as a mechanism for restricting access of subjects to information objects. The paper sets a task of constructing an access control mechanism as a set of functions intended for calculations on each level of the structure of the security domains.

УДК 004.94

ПОЛИМОРФНАЯ ТИПИЗАЦИЯ СУЩНОСТЕЙ И ЗАДАЧА КОНСТРУИРОВАНИЯ МЕХАНИЗМА МНОГОКРИТЕРИАЛЬНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

Р. Г. Бияшев, М. Н. Калимолдаев, О. А. Рог

Институт информационных и вычислительных технологий КН МОН РК, Алматы, Казахстан

Ключевые слова: информационная безопасность, мандатные политики безопасности, многокритериальное разграничение доступа, домен безопасности, теория типов, вычислимые функции.

Аннотация. Рассматриваются вопросы реализации формальной модели системы многокритериального разграничения доступа (МСРД), допускающей одновременное применение ряда моделей безопасности мандатного типа, представленных единым образом, что обеспечивает многоаспектную безопасность доступа субъектов к объектам.

Предложен принцип многокритериального разграничения доступа, основанный на множественной категоризации сущностей, реализуемой в виде их множественной полиморфной типизации. В результате сущность приобретает набор значений, соответствующих категориям, каждой из которых сопоставляется определенная модель безопасности.

Дается алгебраическое определение модели безопасности в виде пары домен безопасности – политика безопасности. Домен безопасности соответствует категории МСРД, структурированной на нескольких уровнях, а политика безопасности представляется в виде набора параметризованных вычислимых функций,

предназначенных для построения домена и задания на нем отношения доступа. Набор таких моделей образует систему типов МСРД, служащую механизмом разграничения доступа субъектов к информационным объектам. Ставится задача конструирования механизма разграничения доступа в виде множества функций, предназначенных для вычислений на каждом из уровней структуризации доменов безопасности.

1. Принцип реализации многокритериального разграничения доступа

Данная статья посвящена вопросам реализации многокритериальной системы разграничения и контроля доступа к информации (МСРД), формальная модель которой представлена в [1, 2].

Большинство моделей безопасности основаны на разделении множества сущностей систем разграничения доступа к информации на субъекты и объекты, и рассмотрении их взаимодействия как элементов с заданными свойствами по правилам определенной политики безопасности. Обозначим E={e} – множество сущностей системы, которое включает подмножества субъектов S={s} и объектов O={o}.

Мандатные политики безопасности, применяемые в настоящее время для разграничения доступа, основаны на присвоении сущностям меток безопасности. Возможность предоставления доступа субъекта к объекту производится путем сравнения значений их меток безопасности и определения доминирования метки безопасности субъекта над меткой безопасности объекта. Для этого на множестве значений меток безопасности устанавливается отношение доминирования в виде отношения порядка.

К сожалению, каждая из известных моделей безопасности мандатного типа, регулируя доступ субъектов к объектам, рассматривает одно свойство сущности в качестве параметра разграничения доступа. Например, модель безопасности Белла и ЛаПадулы основана на предоставлении доступа по значениям уровня конфиденциальности субъектов и объектов. Ролевая модель разграничения доступа (RBAC) разграничивает доступ по видам операций с информационными объектами. Тематическая модель предоставляет доступ на основе принадлежности документа той или иной тематике, организационная – тому или иному отделу организации [3–5].

Разграничения доступа по отдельному признаку недостаточно для отражения реальных ситуаций, имеющих место в условиях функционирования информационных систем, где данные характеризуются рядом разнотипных свойств, требующих учета в качестве параметров разграничения доступа.

В настоящее время поднимается вопрос обеспечения «многосторонней безопасности» («multilateral security») [6], учитывающей все аспекты защиты от несанкционированного доступа в информационных системах. Эту проблему можно решить, разграничивая доступ с одновременным использованием политик безопасности по каждому из критериев и совместно применяя при этом соответствующие модели безопасности в рамках одной системы, что вызывает трудности из-за отсутствия их единообразного представления.

Проблеме единообразного представления моделей безопасности, а также вопросам их сводимости к друг к другу, посвящены такие работы как [7, 8] и ряд других. Следует отметить, что до настоящего времени единая точка зрения на решение этой проблемы отсутствует.

В формальной модели МСРД, с целью обеспечения многоаспектной безопасности, предлагается принцип единообразного представления политик безопасности мандатного типа и соответствующих им моделей, дающий возможность их одновременного применения в рамках одной системы и обеспечивающий разграничение доступа по нескольким критериям.

Единое представление политик безопасности и соответствующих им моделей. Единое представление политик безопасности и соответствующих им моделей безопасности в МСРД осуществляется следующим образом.

Пространство субъектов и объектов, образующее предметную область многокритериальной системы разграничения доступа, классифицируется по различным признакам, таким как отделы, тематика, роли, уровни конфиденциальности, образуя структурные единицы, которые имеют в общем случае иерархическое строение. Согласно своим свойствам, сущность может оказаться принадлежащей нескольким структурным единицам и, следовательно, нескольким классифицирующим категориям, называемым категориями разграничения доступа или категориями безопасности.

Категория МСРД содержит все возможные значения привилегий доступа (атрибутов безопасности, или классификационных атрибутов), которые сущности могут иметь по этой категории. Разрабатываемый вариант МСРД предполагает независимость категорий.

Для обеспечения возможности выполнения мандатных политик безопасности по каждой из категорий сравнением значений привилегий доступа сущностей, множества элементов категорий структурируются единым образом путем задания для каждой категории отношения частичного порядка, представляющего отношение доминирования меток безопасности. Конкретный вид этого отношения зависит от политики безопасности, применяемой для категории.

Таким образом, каждая категория приобретает тип, определяемый как множество элементов категории, упорядоченное в соответствии с применяемой для этой категории политикой безопасности.

Тип категории применяется для классификации сущностей МСРД. Он определяет возможность использования сущности в рамках той или иной политики безопасности средствами соответствующей модели безопасности и служит информационно-логической схемой предметной области этой модели.

Типизация категорий – это динамический процесс, он реализует категоризацию сущностей в МСРД и осуществляется администратором в процессе ***функционирования*** системы разграничения доступа.

Обобщенный тип категории, следуя [9], может быть представлен в виде:

$$T = (D, \leq, Op), \quad (1)$$

где D – домен категории; ≤ – отношение частичного порядка на множестве элементов категории, представляющего на ней отношение доминирования значений меток безопасности. Множество, в частности, может быть неупорядоченным, упорядоченным линейно или упорядоченным иерархически в виде дерева; Op – множество операций с элементами множества D.

Такая организация структуры категории позволяет осуществлять иерархическую группировку привилегий доступа, что обеспечивает:

– передачу прав доступа по уровням структуры категории;

– возможность группового управления привилегиями доступа с учетом иерархической организации пространства субъектов и объектов.

Подвиды структур, образуемых отношением частичного порядка, отражают особенности моделей безопасности.

Например, линейно упорядоченное множество используется в модели Белла и ЛаПадулы.

Скалярное множество подходит для применения в моделях ролевого, тематического или организационного разграничения доступа, категории которых не содержат иерархической группировки названий привилегий доступа.

Эти же модели могут иметь категории, в которых привилегии доступа образуют иерархически вложенные группы. Так, ролевая модель разграничения доступа (RBAC) разграничивает доступ по видам операций и их группам. К числу операций относятся «чтение», «запись», «корректировка». Они могут быть объединены в группы, или роли, такие как «автор», «редактор», «рецензент», «администратор» и т.д. Названия тематик и отделов в тематической и организационной моделях разграничения доступа также допускают иерархическую группировку

Множественная типизация сущности. В соответствии с принадлежностью к определенной категории сущность получает значение метки безопасности в виде привилегии доступа по этой категории, причем для субъекта привилегия доступа выражает его право доступа, а для объекта – вид доступа.

Значение метки безопасности сущности по определенной категории служит своего рода интерфейсом, или ключом доступа данной сущности по категории. Для субъекта оно означает возможность доступа ко всем тем объектам, чьи метки безопасности доминируются меткой безопасности данного субъекта. Для объекта оно означает, что к нему имеют доступ все субъекты, метки безопасности которых доминируют над его меткой безопасности.

При поступлении запроса на доступ от субъекта к объекту, их метки безопасности сравниваются для установления факта доминирования метки безопасности субъекта над меткой безопас-

ности объекта, что означает возможность доступа или выполнение политики безопасности по категории.

Метка безопасности сущности e по категории i определяется д в у м я с п о с о б а м и:

а) e_i – как элемент частично упорядоченного множества категории;

б) $\{e_i\}$ – как подмножество подчиненных ему элементов.

Таким образом, в многокритериальной системе разграничения доступа производится множественная категоризация сущностей, реализуемая в виде их множественной типизации.

Набор значений привилегий, полученный сущностью по всем категориям, образует ее метку безопасности, которая *однозначно определяет* сущность (субъект или объект) в системе разграничения доступа. Метка безопасности сущности в системе также определяется двояко:

а) в виде кортежа элементов категории:

$$e = (e_1, e_2, \ldots, e_n), \quad (2)$$

где e_i – метка безопасности сущности по категории i, заданная в виде элемента категории;

б) в виде кортежа подмножеств элементов категорий:

$$\{e\} = (\{e_1\}, \{e_2\}, \ldots, \{e_n\}), \quad (3)$$

где $\{e_i\}$ – метка безопасности сущности по категории i, заданная в виде подмножества элементов категории, подчиненных элементу e_i; n – число категорий.

Равенства (2)-(3) являются формулировкой механизма типизации сущностей МСРД.

В соответствии с этим на множестве элементов категории i определяется 2 ф о р м ы отношения доминирования метки безопасности субъекта над меткой безопасности объекта:

а) Как отношение иерархического предшествования $\geq$ на множестве элементов категории:

$$s \geq o \Leftrightarrow s \geq o ;$$

б) Как отношение включения подмножеств частично упорядоченного множества элементов категории, подчиненных элементам категории, задающих метки безопасности субъекта и объекта:

$$\{s\} \geq \{o\} \Leftrightarrow \{s\} \subset \{o\} \text{ или } \{s\} \supset \{o\} .$$

Направление оператора включения зависит от политики безопасности для категории.

Категорию можно рассматривать как структурированное множество всевозможных значений меток безопасности сущностей по ней.

Определение механизма разграничения доступа для категории. В [3, 10] показано, что модели безопасности мандатного доступа относятся к классу LBAC (Lattice Based Access Control – метод разграничения доступа, основанный на решетке) и контроль безопасности информационных потоков в них базируется на использовании аппарата решеточно упорядоченных множеств.

Определим обобщенный механизм разграничения доступа для категорий со структурами различных видов. Для этого представим тип категории (1) в виде полной решетки, упорядоченной отношением доминирования меток безопасности способом, указанным в [9, 3]:

$$T_L = (D_L, \leq, Op), \quad (4)$$

где D_L – домен типа категории (1) в виде полной решетки, дополненный элементами T и $\perp$:

$$D_L = D \cup \{Тб \perp\},$$

$\leq$ и Op – указаны в (1).

Символ T помещается в корень дерева элементов категории. В зависимости от контекста операции, он обозначает или максимальный элемент категории или все множество ее элементов. Аналогично, символ $\perp$, на который замыкаются все листовые вершины дерева, обозначает или минимальный элемент категории или пустое множество ее элементов.

При этом появляется возможность задать операции множества Op из (4) для получения точной верхней и точной нижней грани для любой пары сущностей категории i. Эти операции представляют механизм разграничения доступа по категории для пары субъект-объект, представленных значениями своих меток безопасности.

Для значений меток безопасности в виде элементов категории точная верхняя и точная нижняя грани определяются как:

$$MAX(s, o) = \begin{cases} T\,(\text{доступ запрещен}) \\ s, \text{если } s \geq o\ (\text{доступ разрешен}) \end{cases} \quad (5)$$

$$MIN(s, o) = \begin{cases} \top(\text{доступ запрещен}) \\ o, \text{если } s \geq o \ (\text{доступ разрешен}) \end{cases} \quad (6)$$

Для значений меток безопасности в виде подмножеств элементов категории определение точных верхних и нижних граней производится как:

$$MAX(\{s\},\{o\}) = \begin{cases} \top(\text{доступ запрещен}) \\ \{s\}, \text{если } \{s\} \supset \{o\} \mid \{s\} \subset \{o\} \ (\text{доступ разрешен}) \end{cases} \quad (7)$$

$$MIN(\{s\},\{o\}) = \begin{cases} \top(\text{доступ запрещен}) \\ \{o\}, \text{если } \{s\} \supset \{o\} \text{ или } \{s\} \subset \{o\} \ (\text{доступ разрешен}) \end{cases} \quad (8)$$

где направление отношения включения зависит от политики безопасности для категории.

Определенный таким образом механизм разграничения доступа предназначен для реализации политики безопасности МСРД для сущностей определенной категории.

Многокритериальная политика безопасности МСРД. В МСРД, ввиду применения мандатных политик безопасности, предполагается централизованное или принудительное управление доступом, которое означает, что администрирование политик безопасности и привилегий доступа производится специальным выделенным субъектом – администратором, а пользователи лишены возможности изменения и передачи своих прав доступа.

Разграничение доступа субъектов к объектам согласно многокритериальной политике разграничения доступа выполняется следующим образом. При поступлении запроса на доступ от субъекта к объекту, МСРД производит сравнение значений их меток безопасности по каждой из категорий в соответствии с сопоставленными этим категориям политиками безопасности и принимает решение о возможности доступа при условии выполнения политики безопасности для каждой из них.

Разграничение доступа субъектов к объектам происходит в процессе функционирования МСРД, во время выполнения операторов языка определения данных (ЯОД) и языка манипулирования данными (ЯМД). Операторы ЯОД используются для выполнения операций администрирования политик безопасности и прав доступа сущностей, а операторы ЯМД – для предоставления различных видов доступа субъектов к объектам.

В основе работы операторов лежит предикат доступа P = A(s, o), определенный на декартовом произведении множеств значений меток безопасности субъектов и объектов

$$S \times O,$$

где S={s} – множество субъектов, заданных своими метками безопасности:

$$s= (s_1,s_2,\ldots,s_n),$$

O={o} – множество объектов, заданных метками безопасности:

$$o = (o_1,o_2,\ldots o_n),$$

при этом метки безопасности определяются механизмом типизации (2), (3).

Оператор МСРД выполняется, если значение предиката истинно:

$$P \supset \text{Имя\_оператора}(s, o).$$

Для осуществления многокритериальной политики безопасности в МСРД производится:

а) типизация категорий МСРД;

б) динамическая типизация сущностей как объектов разграничения доступа по каждой из категорий. При этом сущности присваивается метка безопасности в виде набора значений различных типов, сопоставленных категориям МСРД;

в) предоставление доступа субъекта к объекту на основании сравнения однотипных значений меток безопасности субъекта и объекта.

Программная реализация многокритериальной политики безопасности МСРД требует конструирования механизма разграничения доступа для каждой из категорий, определенного с помощью (5)-(8), который, по сути, служит реализацией предиката доступа P.

Обобщенное определение модели безопасности для категории. Вышеизложенное позволяет нам дать формальное определение модели безопасности для категории в виде типа категории, а также модели безопасности всей МСРД в виде системы типов МСРД.

Модель безопасности для категории SM_i – строится методом денотационной семантики в виде системы функций, представляющих субъекты и объекты их метками безопасности, и отношения между ними. Эти функции являются средствами динамической типизации категории, выполняя роль политики безопасности для нее.

Модель безопасности для категории i представляет собой пару

$$SM_i = (SD_i, SP_i), \tag{9}$$

где SM_i – модель безопасности для категории; SD_i – домен безопасности для категории. Является декларативным или экстенсиональным представлением типа категории в виде домена типа с заданным на нем отношением частичного порядка; SP_i – политика безопасности для категории. Является процедурным или интенсиональным представлением типа категории в виде множества параметризованных вычислимых функций;

Модель безопасности МСРД, представляющая собой механизм разграничения доступа и одновременно являющаяся ее системой типов, определяется как объединение моделей безопасности для категорий:

$$SM = \bigcup_{i=1}^{n} SM_i .$$

Объектами этой модели служат сущности системы разграничения доступа, однозначно представленные своими метками безопасности.

2. Полиморфное представление системы типов МСРД

Параметр полиморфного представления декларативного и процедурного типов категории (параметр структуризации категории). Система типов многокритериальной системы разграничения доступа (8) обладает свойством параметрического полиморфизма, который позволяет определить входящие в ее состав функции политики безопасности для i-й категории

$$SP_i,\ i= \overline{1,n}$$

таким образом, чтобы вычисления их значений производились идентично вне зависимости от вида структуры типа категории.

Как уже упоминалось, видами структуры множества элементов категории МСРД могут быть подструктуры частично упорядоченного множества, такие как скалярное множество, линейно упорядоченное множество, иерархия в виде дерева.

Для конструирования системы типов МСРД предполагается использовать методику синтаксически ориентированного конструирования типов и функций для их обработки [11]. Следуя специально разработанной для данной методики нотации Ч. Хоара, параметром полиморфного представления системы типов МСРД можно назвать вид структуры категории, диапазон значений которого включает «множество», «список», «дерево».

Структура домена безопасности для категории. Параметрический полиморфизм системы типов дает возможность единообразного представления различных моделей безопасности в многокритериальной системе разграничения доступа.

Домен безопасности SD_i для категории из определения модели безопасности (9) имеет многоуровневую структуру цепочки доменов. Каждый уровень представлен единым для всех категорий образом, зависящим от параметра полиморфного представления типа категории:

$$SD_i = D_i^{Syn} \rightarrow D_i^{Sem} \rightarrow D_i^{SL} \rightarrow B, \tag{10}$$

где D_i^{Syn} – синтаксический домен категории, неструктурированное множество значений привилегий доступа; D_i^{Sem} – семантический домен категории. Является множеством D_i^{Syn}, структурированным в виде полной решетки в соответствии с параметром полиморфного представления типа

категории; D_i^{SL} – домен меток безопасности категории. Представляет собой множество D_i^{Sem} с определенными на нем значениями меток безопасности в соответствии с механизмом типизации (2)-(3). Значения меток безопасности в виде подмножеств сохраняют структуру категории, задаваемую параметром ее полиморфного представления; B – домен булевых значений {истина, ложь}. Его элементы показывают возможность доступа субъекта к объекту, которая определяется с помощью механизма разграничения доступа (5)-(8).

Домен D_i^{SL} является типизированной матрицей доступа категории, представляющей ее область безопасного доступа.

Объединение доменов меток безопасности всех категорий

$$D^{SL} = \bigcup_{i=1}^{n} D_i^{SL}$$

образует типизированную матрицу доступа МСРД, являющуюся областью безопасного доступа МСРД.

3. Система типизации как механизм многокритериального разграничения доступа

Политика безопасности для категории. Формальное представление политики безопасности SP_i из (9) выполняет роль системы типизации для категории. Типизация категорий и сущностей производится динамически, в процессе функционирования МСРД.

Система типизации для категории предназначена для конструирования домена безопасности SD_i из (9) и реализации на нем предиката доступа по категории P_i=A(s,o) в виде механизма разграничения доступа, которое производится с целью обеспечения соблюдения правил политики безопасности для категории.

Формальное выражение политики безопасности SP для всей системы разграничения доступа

$$SP = \bigwedge_{i=1}^{n} SP_i$$

является конъюнкцией формальных выражений механизмов разграничения доступа SP_i по всем категориям. Она обеспечивает соблюдение многокритериальной политики безопасности МСРД.

Система типизации для категории в процессе функционирования МСРД выполняет следующие функции:

а) устанавливает отношение доступа на множестве СЧО при выполнении операторов ЯОД по типизации категорий;

б) проверяет его истинность для пар (s, o) при выполнении операторов ЯМД по предоставлению доступа субъектов к объектам.

При этом система типизации выполняет **задачу** полиморфной структуризации категорий различных видов на всех их уровнях для построения соответствующих категориям доменов безопасности.

Механизм разграничения доступа, реализующий систему типизации для категории, представляется в виде множества вычислимых параметризованных функций, определенных на различных уровнях домена безопасности для категории, определенного в (10). Это множество включает функции для реализации механизма типизации и механизма разграничения доступа по категории.

Политика безопасности для категории задается следующим образом:

$$SP_i = F^{Sem} \rightarrow F^{SL} \rightarrow F^{B},$$

где F^{Sem} – параметрические функции построения семантического домена как абстрактного типа данных с параметром полиморфного представления категории, выполняющие задачу типизации категорий:

$$F^{Sem}: D^{Syn} \rightarrow D^{Sem}$$

F^{SL} – функция уровня безопасности. Присваивает сущности ее метку безопасности. Выполняет задачу типизации субъектов и объектов, определенную механизмом типизации (2), (3):

$$F^{SL}: D^{Sem} \rightarrow D^{SL}$$

F^{B} – функция безопасного доступа. Определяет возможность доступа субъекта к объекту, реализует при этом механизм разграничения доступа, определенный в (5)-(8):

$$F^B: D^{SL} \times D^{SL} \to B$$

Функции SP_i, представляют функциональную программу, вычисляющую значения меток безопасности сущностей как неподвижных точек, и значения отношения доступа между ними в виде значений булевого домена B.

Таким образом, можно сделать вывод о том, что задача построения механизма разграничения доступа МСРД сводится к созданию функциональной программы для реализации системы типизации каждой категории.

Заключение. Показана возможность параметризованного представления моделей безопасности различных видов для их совместного применения в многокритериальной системе разграничения доступа к защищаемым информационным ресурсам.

Строится модель безопасности в виде системы типов МСРД, которая служит реализацией механизма разграничения доступа субъектов к объектам и осуществляет многокритериальную политику безопасности МСРД. Система типов представляется двояко: декларативно – как структура данных и процедурно – как параметризованное множество частично-рекурсивных функций. Эти функции лежат в основе реализации операторов ЯОД и ЯМД МСРД.

Такое представление системы типов дает возможность единообразно типизировать категории различной структуры и осуществлять выполнение соответствующих им политик безопасности.

Построенный механизм является функциональной программой, которая вычисляет значения классификационных атрибутов доменов безопасности для каждой из категорий и принимает решение о предоставлении доступа субъекта к объекту.

Предложенный подход к построению механизма разграничения доступа исключает появление нежелательных информационных потоков, дает возможность группового управления привилегиями доступа по каждой категории, обеспечивает высокую скорость вычислений.

ЛИТЕРАТУРА

[1] Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Формальное представление функциональной модели многокритериальной системы разграничения и контроля доступа к информационным ресурсам // Проблемы информатики. – 2014. – № 1(22). – С. 43-55.

[2] Rog O.A. Polymorphic typing of entities in the multi-criteria system of access control and a task of constructing types. Information Technologies, Management and Society // The 12 th International Scientific Conference Information Technologies and Management. – 2014. April 16–17. – Riga, 2014. – P. 66.

[3] Гайдамакин Н.А. Теоретические основы компьютерной безопасности: учебное пособие. – Екатеринбург: издательство Уральского университета, 2008. – 212 с.

[4] Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2011. – 320 с.

[5] Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство агентства «Яхтсмен», 1996. – 192 с.

[6] Anderson R.J. Security Engineering: a Guide to Building Dependable Distributed Systems. – Wiley Computer Publishing, 2001. – 890 p.

[7] Иткес А.А. Объединение моделей логического разграничения доступа для сложноорганизованных распределенных информационных систем // Проблемы информатики. – 2010. – № 1(5). – С. 85-94.

[8] Zhao G. On The Modeling of Bell-LaPadula Security Policies Using RBAC // Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. – 2008. WETICE '08. IEEE 17th. – 23-25 June 2008. – P. 257-262.

[9] Агафонов В.Н. Типы и абстракция данных в языках программирования (обзор). В Сб. Данные в языках программирования. Абстракция и типология / Пер. с англ.; под ред. В. Н. Агафонова. – М.: Мир, 1982. – 328 с.

[10] Sandhu R.S. Lattice Based Access Control Models // IEEE Computer. – 1993. –Vol. 26, N 11. – P. 9-19.

[11] Душкин Р. Алгебраические типы данных и их использование в программировании // Практика функционального программирования. – 2009. – Вып. 2. – С. 125-157.

REFERENCES

[1] Kalimoldaev M.N., Bijashev R.G., Rog O.A. Formal'noe predstavlenie funkcional'noj modeli mnogokriterial'noj sistemy razgranichenija i kontrolja dostupa k informacionnym resursam. Problemy informatiki. 2014. N 1(22). S. 43-55.

[2] Rog O.A. Polymorphic typing of entities in the multi-criteria system of access control and a task of constructing types. Information Technologies, Management and Society. The 12 th International Scientific Conference Information Technologies and Management. 2014. April 16–17. Riga, 2014. P. 66.

[3] Gajdamakin N.A. Teoreticheskie osnovy komp'juternoj bezopasnosti: uchebnoe posobie. Ekaterinburg: izdatel'stvo Ural'skogo universiteta, 2008. 212 s.

[4] Devjanin P.N. Modeli bezopasnosti komp'juternyh sistem. Upravlenie dostupom i informacionnymi potokami. Uchebnoe posobie dlja vuzov. M.: Gorjachaja linija-Telekom, 2011. 320 s.
[5] Grusho A.A., Timonina E.E. Teoreticheskie osnovy zashhity informacii. M.: Izdatel'stvo agentstva «Jahtsmen», 1996. 192 s.
[6] Anderson R.J. Security Engineering: a Guide to Building Dependable Distributed Systems. Wiley Computer Publishing, 2001. 890 p.
[7] Itkes A.A. Ob#edinenie modelej logicheskogo razgranichenija dostupa dlja slozhnoorganizovannyh raspredelennyh informacionnyh sistem. Problemy informatiki. 2010. N 1(5). S. 85-94.
[8] Zhao G. On The Modeling of Bell-LaPadula Security Policies Using RBAC. Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. 2008. WETICE '08. IEEE 17th. 23-25 June 2008. P. 257-262.
[9] Agafonov V.N. Tipy i abstrakcija dannyh v jazykah programmirovanija (obzor). V Sb. Dannye v jazykah programmirovanija. Abstrakcija i tipologija. Per. s angl.; pod red. V. N. Agafonova. M.: Mir, 1982. 328 s.
[10] Sandhu R.S. Lattice Based Access Control Models. IEEE Computer. 1993. Vol. 26, N 11. P. 9-19.
[11] Dushkin R. Algebraicheskie tipy dannyh i ih ispol'zovanie v programmirovanii. Praktika funkcional'nogo programmirovanija. 2009. Vyp. 2. S. 125-157.

БОЛМЫСТАРДЫ ПОЛИМОРФТЫ ТИПТЕНДІРУ ЖӘНЕ КӨПКРИТЕРИАЛДЫ ҚОЛЖЕТІМДІЛІКТІ ШЕКТЕУ МЕХАНИЗМІН ҚҰРАСТЫРУ ЕСЕБІ

Р. Г. Бияшев, М. Н. Қалимолдаев, О. А. Рог

Тірек сөздер: ақпараттық қауіпсіздік, қауіпсіздіктің мандатты саясаты, көпкритериалды қолжетімділікті шектеу, қауіпсіздік домені, типтер теориясы, есептелінетін функциялар.

Аннотация. Субъектінің объектіге қолжетімділіктің көпаспектілі қауіпсіздігін қамсыздандыратын, бірыңғай түрде көрсетілген, мандатты типтегі қауіпсіздік моделдер қатарын бір уақытта қолдану мүмкіндігі бар, көпкритериалды қолжетімділікті шектеу жүйесінің формалды моделін (ҚШЖМ) жүзеге асыру мәселелері қарастырылып отыр.

Болмыстарды көптік категоризациялау негізінде, олардың көптік полиморфты типизация түрінде жүзеге асырылатын, көпкритериалды қолжетімділікті шектеу принципі ұсынылған. Нәтижесінде болмыс әрқайсысы белгілі бір қауіпсіздік моделі безбендірілетін, категорияларға сәйкес, мәндер жиынын қабылдайды.

Қауіпсіздік саясаты – қауіпсіздік доменінің жұп түріндегі, қауіпсіздік моделінің алгебралық анықтамасы беріледі. Бірнеше деңгейде құрылымдалған, қауіпсіздік домені ҚШЖМ категориясына сәйкес келеді, ал қауіпсіздік саясаты домен құрастыру және ондағы қолжетімділік қатынасын белгілеуге арналған параметрленген есептелінетін функциялар жиыны түрінде ұсынылады. Осындай моделдер жиыны, ақпараттық объектіге субъектілердің қолжетімділігін шектеу механизмі ретінде қызмет ететін ҚШЖМ типтер жүйесін құрайды. Функция жиыны түріндегі, қауіпсіздік доменін құрылымдаудың әр деңгейінде есептеуге арналған, қолжетімділікті шектеу механизмін құрастыру мақсаты қойылып отыр.

Поступила 01.10.2014 г.