REPORTS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
ISSN 2224-5227
Volume 3, Number 313 (2017), 48 – 54

M.N. Kalimoldayev, R.G. Biyashev, O.A.Rog

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

APPLICATION OF LOGIC FOR ACCESS CONTROL MODELING

Abstract. In this article we consider issues concerning access control systems design and construction by means of mathematical logic. The basic currently used principles of their organization in the form of logical systems are given. Their functioning consists in logical proof of various statements which arise during the process of authorized access. These statements are being proved through the deductive apparatus of the appropriate formal theories.

Some aspects of the logic application to access control accepted in the world practice are viewed. A logical system for representing of the currently developed model of the typed attribute based access control is described.

Keywords: information security, logical calculus, deductive apparatus, access control policy, specification language, typed attribute based access control, formal theory.

УДК 004.94.056.53

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

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

ПРИМЕНЕНИЕ ЛОГИКИ ДЛЯ ПОСТРОЕНИЯ МОДЕЛЕЙ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ

Аннотация. Данная статья рассматривает вопросы построения систем разграничения доступа, предоставляющих права и возможности доступа пользователям к информационным ресурсам с использованием аппарата математической логики.

Приводятся основные принципы их организации в виде логических систем, используемые в настоящее время. Их функционирование заключается в логическом доказательстве различных утверждений, возникающих в процессе организации авторизированного доступа посредством дедуктивного аппарата формальных теорий.

Рассматриваются аспекты применения логики для разграничения доступа, принятые в мировой практике. Приводится описание логической системы для представления разрабатываемой в настоящее время модели типизированного атрибутного разграничения доступа.

Ключевые слова: защита информации, логические исчисления, дедуктивный аппарат, политики разграничения доступа, языки спецификаций, типизированное атрибутное разграничение доступа, формальная теория.

1. Введение

Разграничение доступа является ключевым моментом в обеспечении информационной безопасности, затрагивая при этом многие аспекты компьютерных систем. Оно используется в приложениях, виртуальных машинах, операционных системах и сетях.

На первый взгляд, обеспечение доступа к информационным ресурсам только авторизованных пользователей кажется простым, на практике же оно является запутанным и подверженным ошибкам процессом, а многие его механизмы оказываются неэффективными.

Широкое распространение распределенных систем диктует дополнительную необходимость учета особенностей вычислительных сред, характеризующихся масштабностью, открытостью,

пространственной локализацией и неоднородностью, в то же время обладающих единым пространством имен и требованиями глобальной безопасности. При этом вычислительная база распределенной системы не обязательно должна располагаться в единственном месте под единым управлением. При организации разграничения доступа в таких средах требуется обеспечивать их связность и интеграцию неоднородных участков.

Языки для описания современных процессов разграничения доступа к защищаемым ресурсам должны быть гибкими и расширяемыми, обладать достаточными выразительными возможностями для представления политик безопасности.

С другой стороны, использование таких развитых языков как, например, XACML или WS-Policy, вызывает трудности полного понимания администраторами по безопасности всех эффектов от применения той или иной политики разграничения доступа. Простая проверка факта, что политика не вызовет утечки привилегий к неавторизованным сущностям, проводимая вручную, является кропотливым и ненадежным процессом. Исправление ошибок в описании политики может привести к другим неточностям и появлению новых брешей в безопасности.

Список требований, предъявляемых к языкам описания политик разграничения доступа, включает их способность описывать разнородные политики безопасности, разрешение конфликтов, формальное представление семантики.

Необходимо наличие возможности автоматической проверки политик, представляемых языками, на избыточность, совместимость, согласованность. Политики должны быть настраиваемыми, иметь полный охват субъектов и объектов, а также их полномочий.

Учет полного спектра перечисленных требований возможен только в больших и сложных системах разграничения доступа, имеющих в своей основе теоретическую базу и программный инструментарий поддержки процессов проектирования коллективного доступа к разделяемым информационным ресурсам, составляющих методологический фундамент для их всестороннего анализа и исследования [1].

В связи с этим многие исследователи в качестве основы для языков описания политик разграничения доступа предлагают использование методов математической логики. Ожидается, что логика окажется простым, надежным и общим формальным основанием разграничения доступа, предоставив при этом средства для проектирования, реализации и верификации различных его механизмов. Исследования последнего времени показывают, что, хотя логику и нельзя считать панацеей, ее вклад в организацию разграничения доступа является существенным и полезным.

Языки спецификаций политик разграничения доступа строятся в виде исчислений, объектами которых являются различные сущности разграничения доступа. Политики в них представляются посредством правил, которые выполняют логические выводы относительно значений привилегий участников, возможности их доступа к ресурсам, обеспечивают разрешение конфликтов, а также проверку ограничений целостности [2].

В основу построения языков помещаются логические системы, содержащие дедуктивный аппарат для доказательства теорем относительно процесса разграничения доступа, среди которых главным является ответ на вопрос о возможности предоставления доступа субъекта к объекту.

Логики позволяют описывать протоколы и политики на разумном уровне абстракции, что важно в контексте гетерогенных распределенных сред, где одновременно могут существовать различные реализации одной и той же модели. Становится возможным строить ряд существующих моделей разграничения доступа путем конструирования их логик в виде отдельных наборов аксиом и правил вывода.

Представление языков спецификации политик безопасности в виде логических систем ставит процесс разграничения доступа на теоретическую основу, позволяя применять аппарат автоматического доказательства теорем для автоматической верификации процесса авторизации и обеспечения безопасности информационных ресурсов [3, 4].

В данной статье кратко рассматриваются принципы применения логики для построения моделей различных видов разграничения доступа, применяемые в настоящее время на практике, и системы разграничения доступа на их основе. Обсуждаются преимущества и недостатки этого подхода.

Приводится описание логической системы для представления модели типизированного атрибутного разграничения доступа, разрабатываемой в настоящее время авторами статьи. Основой логической системы служит логика предикатов 1-го порядка, построенная на специальным образом организованной теории типов атрибутов безопасности, которая дает ее одновременное представление в виде логики 2-го порядка, что делает возможной иерархическую структуризацию пространства сущностей в процессе выполнения, устанавливающую ряд отношений в виде отношения доступа (субъект, объект), и отношений иерархического предшествования (субъект, субъект) и (объект, объект). Подобный подход позволяет осуществить реализацию модели на языках логического и функционального программирования.

2. Логика как основа разграничения доступа

Разграничение доступа основано на субъектно-объектной модели. Оно заключается в принятии решения о возможности доверия субъекту, выдавшему запрос на доступ к определенному объекту. При этом субъектом, например, может считаться процесс, запущенный пользователем, запросом – команда чтения, а объектом – файл.

Типичными компонентами триады для представления систем разграничения доступа на разных уровнях абстракции являются политика разграничения доступа, ее модель и ее механизм.

Политика разграничения доступа определяется как высокоуровневые неформальные предписания, регулирующие порядок доступа субъектов к объектам. Критериями разграничения доступа при этом могут быть использование ресурсов в пределах одной или нескольких организаций, уровни конфиденциальности, компетентности, обязательства, конфликты интересов.

Модель представляет собой описание политики на одном из формальных языков, который при этом считается языком спецификации политики разграничения доступа. Механизмы служат для реализации политик в виде программ, зависящих от вычислительных сред, в которых функционируют системы разграничения доступа. С помощью механизмов представляются матрицы доступа, отображающие имена объектов и субъектов на множество разрешенных операций. Реализуются матрицы доступа в виде списков контроля доступа, приписываемых объектам или списков возможностей, которыми обладают субъекты. В случае необходимости принимать решения о возможности доступа при наличии сложных условий, например, принадлежности пользователя группе, в качестве матриц доступа используются сложноструктурированные области – «отношения авторизации» [3].

Предметной областью разграничения доступа называется фиксированная совокупность субъектов и объектов, их свойств и взаимоотношений между ними.

Для решения задач в области организации разграничения доступа требуется обеспечить точную спецификацию потребностей защиты в виде политик разграничения доступа. Что должно защищаться и от кого, каким образом обозначать то, что авторизовано или запрещено, как доказывать безопасность приложений и систем. Ответы на эти вопросы могут быть получены путем применения языков и дедуктивных аппаратов разнообразных логических систем, конструируемых для объектов разных видов с учетом требований конкретных задач.

Основной концепцией при этом считается, что разграничение доступа принципиально сводимо к формальной логике. При этом многие его аспекты могут быть сформулированы в терминах некоторого символического языка и распознаваться как логические истины, а математические доказательства вопросов о возможности доступа представляться как цепи логического вывода [5].

Языки спецификации политик разграничения доступа, основанные на логике, обладают неизбыточной семантикой, вычислимостью, допускающей формальную верификацию, достаточно выразительны для представления всех видов политик безопасности, известных в настоящее время. Они имеют высокий уровень абстракции, приближающий их к естественным языкам. С их помощью становится возможным конструировать политики безопасности, в том числе динамические, представлять иерархии и наследование групп сущностей, обрабатывать исключительные ситуации и управлять сообщениями.

Модели разграничения доступа, представленные в виде логических систем, имеют вид:

$$LS = (L, Ax, Inf),$$

где L=(A, G) – язык, со множеством символов определенного алфавита A и правилами грамматики G, с помощью которых конструируются формулы. Ax – схема аксиом, в качестве которых используется определенное множество формул, Inf – набор правил вывода для получения теорем. Синтаксис спецификаций политики разграничения доступа задается языком L, а семантика генерируется путем применения аксиом и правил вывода. Аксиомы и правила вывода образуют дедуктивный аппарат логической системы, который предназначен для формирования матрицы доступа во время функционирования системы разграничения доступа.

В настоящее время существуют две основные модели разграничения доступа: дискреционная (DAC) и мандатная (MAC), а также ролевая (RBAC), сочетающая черты их обеих. Неудобство этих моделей, обеспечивающих разграничение доступа по одному критерию, вызывает многочисленные нарекания, что инициировало разработки так называемого атрибутно-ориентированного разграничения доступа (ABAC). Согласно ABAC, объекты и субъекты снабжаются наборами атрибутов, которые подвергаются оценке в соответствии с заданными правилами, определяющими возможность доступа. В обзорах [2, 3, 6, 7] приводятся многочисленные примеры различных путей применения логики в системах разграничения доступа, использующих перечисленные виды моделей.

Однако, как отмечается в [3], несмотря на значительный вклад логики в конструирование и исследование языков и систем разграничения доступа, она не смогла полностью заменить традиционные механизмы разграничения доступа и нет надежды, на то, что это произойдет в ближайшем будущем.

3. Логика типизированного атрибутного разграничения доступа

Типизированное атрибутное разграничение доступа (ТАРД), разрабатываемое авторами статьи, основано на понятии типа атрибутов субъектов и объектов. Оно является вариантом ABAC, наследующим преимущества и преодолевающим большинство из его недостатков. В работах [8-13] изложены концепции ТАРД и приводятся алгебраические спецификации метамодели ТАРД, на базе которой могут быть получены конкретные модели разграничения доступа, такие как DAC, MAC, RBAC, основанные на определенном типе атрибутов, и осуществляющие разграничение доступа по признакам, задаваемым этим типом.

Модель типизированного атрибутного разграничения доступа определяется в виде типа атрибутов, задаваемого следующим образом [13]:

$$T=(D, \sigma),$$

где $D=(A, \sqsubseteq)$ – домен всевозможных значений атрибутов A, структурированный в виде полной решетки, упорядоченной отношением частичного порядка $\sqsubseteq$;

$\sigma=\{SL, SL1, Acc\}$ – многосортная сигнатура набора операций и предикатов. $Sort=\{D, B\}$-множество сортов (типов) аргументов и значений этих операций. Среди них $B=\{true, false\}$ - булев тип.

Субъектно-объектная модель ТАРД содержит множество сущностей $E=\{e\}$, $E=SUO$, $S=\{s\}$-субъекты, а $O=\{o\}$-объекты разграничения доступа.

Политика типизированного атрибутного разграничения доступа выражается формально с помощью операций σ:

Операция типизации SL: $D\rightarrow D$ присваивает сущности метку безопасности в виде атрибута $a\in A$ типа T.

Операция типизации SL1: $D\rightarrow P(D)$ присваивает сущности метку безопасности в виде подмножества атрибутов $SL1(a)=\{a_i | a_i \sqsubseteq a, a_i \in A\}$ типа T.

Операция сравнения атрибутов Acc: $(D\rightarrow D)\rightarrow B$ осуществляет сравнение однотипных меток безопасности, разрешая/отвергая возможность доступа субъекта к объекту:

Acc(SL(s), SL(o)) = true/false или Acc(SL1(s), SL1 (o)) = true/false.

Представим модель типизированного атрибутного разграничения доступа T в виде логической системы (или логики) $LS_T = (L_T, Ax_T, Inf_T)$, в которой язык L_T задает синтаксис языка спецификации политик типизированного атрибутного разграничения доступа, а набор аксиом Ax_T и правила вывода Inf_T – его семантику.

Логическая система LS_T, представленная на уровнях

Металогика ММ → Объектная логика OL → Матрица доступа АМ служит основой для построения систем, в которых возможно одновременное применение различных моделей безопасности, объединяемых единообразной обработкой типизированных атрибутов разграничения доступа. При этом обеспечивается возможность формального доказательства безопасного доступа субъектов к объектам путем логического вывода теорем.

Металогика, представленная в виде тройки (L, Ax, Inf), выглядит следующим образом:

$$MM = (L_{MM}, Ax_{MM}, Inf_{MM}),$$

где $L_{MM} = (A_{MM}, G_{MM})$ – язык металогики с алфавитом A_{MM}=((NUVUTU⊥)) и правилами грамматики G_{MM}.

A_{MM}=(NUVUTU⊥) – алфавит языка. N={n}–множество переменных языка, представляющих имена атрибутов, V={v}–множество переменных языка, представляющих значения атрибутов. N∩V=∅. По крайней мере одно из множеств N или V не пусто. A_{MM} является полной решеткой с отношением частичного порядка $\sqsubseteq_{MM}$. T служит в ней наибольшим элементом, а элементы множества V или множества {⊥} (в случае V=∅) – минимальными элементами.

G_{MM} = {SL, SL1} – правила грамматики языка, порождающие цепочки символов атрибутов, образующих метки безопасности субъектов и объектов.

Ax_{MM} = {SL(e)=a ∀a∈ $A_{MM;}$; SL1(e)={a, a_i}, $a_i \sqsubseteq_{MM}$ a, где a,a_i∈A_{MM} ∀i} – система аксиом металогики в виде множества значений меток безопасности сущностей.

Inf_{MM} = {Acc} – правило вывода металогики, согласно которому на основании значений меток безопасности доказывается теорема, или делается вывод о возможности предоставления доступа субъекта к объекту.

Как было показано в [12, 13], в силу своего определения, структура решетки домена типа T, представляющего модель ТАРД, так же как и структура решетки множества A_{MM}, представляющего алфавит металогики ММ, позволяют выделить следующие подструктуры: S - в виде скалярного множества, Li – линейно упорядоченного множества и Tr – в виде дерева. В соответствии с этим, металогика ММ порождает объектные логики OL_I , которые являются конкретными моделями разграничения доступа разных видов:

$$OL_I = (L_I, Ax_I, Inf_I).$$

I∈{S, Li, Tr} – индекс структуризации. I=S служит для создания моделей типа MAC, I=Li – моделей MAC, а I=Tr моделей RBAC.

$L_I = (A_I, G_I)$ –язык объектной логики. Алфавит A_I образуется из алфавита A_{MM} путем присвоения элементам N и V конкретных значений атрибутов, формируя множество констант языка. $G_I = \{SL_I, SL1_I\}$ – правила грамматики в виде функций, имеющих конкретный вид, необходимый для обработки элементов множества структуры I. Таким образом, с помощью языка L_I происходит формирование определенной модели типизированного атрибутного разграничения доступа в виде домена типа атрибутов с заданными на нем операциями.

Ax_I – аксиомы логики OL_I, представляющие собой метки безопасности сущностей, создаваемые функциями SL_I, $SL1_I$.

$Inf_I = \{Acc_I\}$ – правило вывода логики L_I, осуществляющего сравнение меток безопасности субъекта и объекта по правилам, диктующим обработку элементов домена типа структуры I.

В процессе функционирования системы типизированного атрибутного разграничения доступа логическая система OL_I формирует матрицу доступа AM_I соответствующей структуры, которая также является логической системой:

$$AM_I = (L^I_{AM}, Ax^I_{AM}, Inf^I_{AM}).$$

$L^I_{AM} = Ax^I_{AM}$ – язык, представленный множеством цепочек, генерируемых функциями SL_I и $SL1_I$. Они же образуют множество аксиом $Ax^I_{AM.}$

AM_I является сложноструктурированной средой хранения меток безопасности сущностей, образованных значениями их атрибутов. Анализируя эти значения, система типизированного атрибутного разграничения доступа с помощью правила вывода $Inf^I_{AM}=Acc_I$ делает выводы о возможности доступа субъектов к объектам.

Представление модели типизированного атрибутного разграничения доступа в виде логической системы позволяет формально доказывать правильность присвоения привилегий сущностям и корректность работы системы, обеспечивая безопасный доступ субъектов к объектам. Многоуровневость модели обеспечивает возможность создания ее различных вариантов, совместное применение которых в рамках одной системы позволяет осуществлять разграничение доступа по нескольким критериям одновременно.

Наконец, модель типизированного атрибутного разграничения доступа в виде логики непосредственно реализуема на языках логического и функционального программирования.

Заключение

Рассмотрены методы математической логики, используемые для построения систем разграничения доступа.

Приводятся особенности их работы, анализируются преимущества и недостатки. Описана логическая система, представляющая модель типизированного атрибутного разграничения доступа.

ЛИТЕРАТУРА

[1] Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах / – Екатеринбург: Изд-во Урал. ун-та, 2003 . – 328 с.

[2] Kolovski V. Logic -based access control policy specification and management (2007). Available at https://pdfs.semanticscholar.org/a3a9/1ed804dc5e2d589cccc5cc407eef3f47e46e.pdf

[3] Abadi M. (2009). Logic in Access Control (Tutorial Notes). In Foundations of Security Analysis and Design V, Alessandro Aldini, Gilles Barthe, and Roberto Gorrieri (Eds.). Lecture Notes In Computer Science, Vol. 5705. Springer-Verlag, Berlin, Heidelberg 145-165. DOI=http://dx.doi.org/10.1007/978-3-642-03829-7_5

[4] Abadi M., Burrows M., Lampson B., Plotkin G. (1993). A calculus for access control in distributed systems. *ACM Trans. Program. Lang. Syst.* 15, 4 (September 1993), 706-734. DOI=10.1145/155183.155225 http://doi.acm.org/10.1145/155183.155225

[5] Bonatti P.A., Samarati P. Logics for authorization and security. In: Logics for Emerging Applications of Databases, pp. 277-323. Springer, Heidelberg (2003)

[6] *Damianou N., Bandara A., Sloman M., Lupu E. A survey of policy specification approaches, "Department of Computing, Imperial College of Science Technology* and Medicine, London", 3, 142-156, 2002

[7] Biswas P., Sandhu R., Krishnan R. A Comparison of Logical Formula and Enumerated Authorization Policy ABAC Models Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec '16), Trento, Italy, July 18-21, 2016

[8] 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.

[9] 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. - с. 66.

[10] Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Полиморфная типизация сущностей и задача конструирования механизма многокритериального разграничения доступа. // Известия НАН РК. Серия физико-математическая. – 2014. – № 5. – С. 33-41.

[11] Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Логический подход к организации многокритериального атрибутного разграничения доступа. // Совместный выпуск по материалам международной научной конференции «Вычислительные и информационные технологии в науке, технике и образовании» (CITech-2015) (24-27 сентября 2015 г.) Вычислительные технологии т.20, Вестник КазНУ им. Аль-Фараби, серия математика, механика и информатика №3(86) Часть 1. - С.275-278.

[12] Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Представление ограничений моделей атрибутного разграничения доступа // Известия НАН РК. Серия физико-математическая. – 2016. – № 1. – С. 58-65.

[13] Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Моделирование семантики типизированного атрибутного разграничения доступа // журнал Проблемы информатики, 2017, № 1. С. 25-37.

REFERENCES

[1] Gajdamakin N.A. Access control in computer systems *Ekaterinburg : Izd-vo Ural. un-ta*, **2003** . 328 s. (in Russ.).

[2] Kolovski V. Logic -based access control policy specification and management **(2007)**. Available at *https://pdfs.semanticscholar.org/a3a9/1ed804dc5e2d589cccc5cc407eef3f47e46e.pdf* (in Eng.).

[3] Abadi M. **(2009)**. Logic in Access Control (Tutorial Notes). In *Foundations of Security Analysis and Design V, Alessandro Aldini, Gilles Barthe, and Roberto Gorrieri (Eds.). Lecture Notes In Computer Science*, Vol. 5705. Springer-Verlag, Berlin, Heidelberg 145-165. DOI=http://dx.doi.org/10.1007/978-3-642-03829-7_5 (in Eng.).

[4] Abadi M., Burrows M., Lampson B., Plotkin G. **(1993)**. A calculus for access control in distributed systems. *ACM Trans. Program. Lang. Syst.* 15, 4 (September 1993), 706-734. DOI=10.1145/155183.155225 http://doi.acm.org/10.1145/155183.155225 (in Eng.).

[5] Bonatti P.A., Samarati P. Logics for authorization and security. In: *Logics for Emerging Applications of Databases*, pp. 277-323. Springer, Heidelberg **(2003)** (in Eng.).

[6] *Damianou N., Bandara A., Sloman M., Lupu E. A survey of policy specification approaches,* Department of Computing, Imperial College of Science Technology *and Medicine, London*, 3, 142-156, **2002** (in Eng.).

[7] Biswas P., Sandhu R., Krishnan R. A Comparison of Logical Formula and Enumerated Authorization Policy ABAC Models *Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec '16)*, Trento, Italy, July 18-21, **2016** (in Eng.).

[8] Kalimoldaev M.N., Bijashev R.G., Rog O.A. Formal representation of the functional model of multi-criteria access control system *Problemy informatiki*. 2014. № 1(22). S. 43-55. **(in Russ.).**

[9] 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. c. 66.

[10] Bijashev R.G., Kalimoldaev M.N., Rog O.A. Polymorphic typing of entities and a task of constructing of the multi-criteria access control mechanism *Izvestija NAN RK. Serija˙fiziko-matematicheskaja*. **2014. № 5. S. 33-41.** (in Russ.).

[11] Bijashev R.G., Kalimoldaev M.N., Rog O.A. A logical approach to organization of the multi-criteria attribute-based access control *Sovmestnyj vypusk po materialam mezhdunarodnoj nauchnoj konferencii «Vychislitel'nye i informacionnye tehnologii v nauke, tehnike i obrazovanii»* (CITech-2015) (24-27 sentjabrja **2015** g.) *Vychislitel'nye tehnologii t.20, Vestnik KazNU im. Al'-Farabi, serija matematika, mehanika i informatika* №3(86) Chast' 1. S.275-278. (in Russ.).

[12] Bijashev R.G., Kalimoldaev M.N., Rog O.A. Constraint representation in the attribute-based access control models *Izvestija NAN RK. Serija˙fiziko-matematicheskaja*. 2016. № 1. S. 58-65. (in Russ.).

[13] Bijashev R.G., Kalimoldaev M.N., Rog O.A. Typed attribute-based access control semantics modeling *Zhurnal Problemy informatiki*, **2017**, № 1. S. 25-37. (in Russ.).

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

ҚР БжҒМ ҒК Ақпараттық және есептеу технологиялар институты, Алматы, Қазақстан

АҚПАРАТҚА ҚОЛ ЖЕТКІЗУ САРАЛАУ ҮЛГІСІН ҚҰРУ ҮШІН ЛОГИКАСЫН ПАЙДАЛАНЫҢЫЗ

Аннотация. Бұл мақалада математикалық логика пайдалана ақпараттық ресурстарға пайдаланушылардың қол құқықтары мен мүмкіндіктерін қамтамасыз ету, кіруді бақылау жүйесін құру мәселелерін қарастырады.

Қазіргі уақытта пайдалану логикалық жүйелер түрінде олардың ұйымдастырудың негізгі принциптері. Олардың операция ресми теориялар дедуктивті аппаратының арқылы уәкілетті қол ұйымдастыру туындауы түрлі шағымдар логикалық дәлелі болып табылады.

Катынасты басқару үшін бағдарлама логика аспектілері, әлемдік тәжірибеде қабылданған. Атрибут кіруді бақылау терілген қазіргі дамыған модельдерін ұсыну үшін логикалық жүйесін сипаттау.

Тірек сөздер: деректерді қоргау, логикалық есептеу, дедуктивті аппараты, қатынасты басқару саясаты, ерекшелігі тілдері, атрибут кіруді бақылау терілген, ресми теориясы.

Сведения об авторах:

Калимолдаев Максат Нурадилович - д-р физ.-мат. наук, член-корр. НАН РК, генеральный директор Института информационных и вычислительных технологий КН МОН РК; e-mail: mnk@ipic.kz;

Бияшев Рустем Гакашевич - д-р техн. наук, заведующий лабораторией Института информационных и вычислительных технологий КН МОН РК; e-mail: brg@ipic.kz;

Рог Ольга Алексеевна - н.с. Института информационных и вычислительных технологий КН МОН РК; e-mail: olga@ipic.kz