Саломатин Александр Александрович – Институт проблем управления им. В.А. Трапезникова РАН; e-mail: sandr@ipu.ru; г. Москва, Россия, тел.: 84953348910; лаборатория Киберфизических систем; к.т.н.; с.н.с.

Bogacheva Darya Nikolaevna – V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences; e-mail: bogacheva@ipu.ru; Moscow, Russia; phone: +74953348910; Infrastructure Systems Laboratory; junior researcher.

Lukinova Olga Vasilievna – V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences; e-mail: lukinova@ipu.ru; Moscow, Russia; phone: +74953348910; Infrastructure Systems Laboratory; dr. of eng. sc.; associate professor; leading researcher.

Salomatin Aleksandr Aleksandrovich – V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences; e-mail: sandr@ipu.ru; Moscow, Russia; phone: +74953348910; Cyber-Physical Systems Laboratory; cand. of eng. sc.; senior researcher.

УДК 004.056.53:004.75 DOI 10.18522/2311-3103-2026-1-179-191

Д.О. Ларин, Р.И. Захарченко, С.А. Диченко

МАНДАТНАЯ АТРИБУТИВНО-РОЛЕВАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ В КРУПНОМАСШТАБНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

В условиях стремительного развития информационных систем федерального масштаба, их эволюции в цифровые экосистемы, к процессу обеспечения безопасности обрабатываемой в них информации предъявляются новые требования. Такими требованиями, в частности, являются повышение доступности информации при управлении доступом пользователей с сохранением требуемого уровня ее конфиденциальности, принятие решения о доступе к ресурсам на основе множества факторов. Для их удовлетворения ранее было предложено множество композиционных моделей управления доступом на основе ролей и атрибутов, которые решили ряд актуальных проблем, сохранив удобство администрирования и обеспечив при этом гибкость и масштабируемость без «взрыва ролей». Однако известные модели все еще имеют существенный недостаток – невозможность их использования в информационных системах, где обрабатывается информация высокого уровня значимости. Целью исследования является разработка в рамках методологии субъект-сущностного подхода теории информационной безопасности новой мандатной атрибутивно-ролевой модели управления доступом, а также ее формальное описание с помощью математического аппарата теории автоматов. Использование модели позволит предотвращать запрещенные информационные потоки от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности динамически, в процессе ограничения набора разрешений, назначенных роли, с помощью реализации мандатного разграничения доступа через отдельную атрибутивную политику, сохраняя при этом возможность предоставления пользователям доступа высокой степени детализации на основе атрибутов контекста. Применение модели может быть востребовано в крупномасштабных информационных системах, где одновременно обрабатывается информация различных уровней конфиденциальности и, ввиду особенностей функционирования, необходима реализация атрибутивного управления доступом.

Атрибутивное управление доступом; ролевое управление доступом, мандатное управление доступом; модель управления доступом; MAP модель; конфиденциальность; доступность.

D.O. Larin, R.I. Zaharchenko, S.A. Dichenko

MANDATORY ROLE-CENTRIC ATTRIBUTE-BASED ACCESS CONTROL MODEL FOR LARGE-SCALE INFORMATION SYSTEMS

In the context of the rapid development of national-scale information systems and their evolution into digital ecosystems, new requirements are imposed on the process of ensuring the security of the information processed within them. These requirements include enhancing information availability in user access management while maintaining the required level of confidentiality, and making access decisions to resources based on multiple factors. To meet these requirements, numerous compositional access control models based on roles and attributes have been proposed previously, which have resolved several pressing issues while maintaining administrative convenience and providing flexibility and scalability

without role explosion. However, known models still have a significant limitation – the impossibility of their use in information systems where high-sensitivity data is processed. The aim of the study is to develop, within the framework of the subject-object approach methodology in information security theory, a new mandatory role-centric attribute-based access control (MRABAC) model, as well as its formal description using the mathematical apparatus of automata theory. The use of the model will enable dynamic prevention of unauthorized information flows from high-confidentiality objects to low-confidentiality objects during the restriction of the permission set assigned to a role, through the implementation of mandatory access control via a separate attribute-based policy, while preserving the ability to provide users with fine-grained access based on contextual attributes. The application of the model may be particularly useful in large-scale information systems where information of various confidentiality levels is processed simultaneously, and, due to operational characteristics, attribute-based access control is necessary.

Attribute-based access control; role-based access control; mandatory access control; access control model; MRABAC; confidentiality; availability.

Введение. Сегодня основой деятельности как крупных частных компаний, так и целых отраслей государства являются крупномасштабные информационные системы (КМИС), появление которых стало возможным благодаря развитию технологий распределенных вычислений, облачных вычислений, мобильного интернета, интернета вещей. Стремительная эволюция КМИС и их особенности, такие, как большой территориальный размах; многоуровневая иерархическая структура; многоцелевой характер функционирования; разнородность и сложное взаимодействие элементов (информационных ресурсов и систем); огромное количество пользователей, динамический характер их поведения и информационных потребностей [1] порождают необходимость в разработке новых и совершенствовании существующих способов обеспечения безопасности информации и, в частности, моделей и методов управления доступом.

В отличие от информационных систем (ИС) объектового масштаба (одна организация или предприятие), где количество субъектов и объектов доступа ограниченно, а требования к управлению доступом статичны и могут быть легко удовлетворены такими классическими моделями управления доступом, как дискреционного (DAC) [2], мандатного (MAC) [3] и ролевого (RBAC) [4] управления доступом или их композицией [5, 6], в современных гетерогенных КМИС доступ зависит от множества факторов, так называемого контекста (context-aware access), в котором поступают запросы на доступ – различных атрибутов субъектов (специализация, возраст, гражданство и др.), объектов (тип, статус, принадлежность владельцу и др.) и среды (местоположение пользователя, время его обращения и др.), и обеспечение такого гибкого доступа выходит за рамки возможностей этих моделей.

Исходя из новых требований к обеспечению доступа пользователей к ресурсам была разработана и принята в качестве стандарта модель атрибутивного управления доступом (ABAC/XACML) [7, 8], которая успешно решает известную проблему «взрыва ролей» модели RBAC и обеспечивает динамическое, детализированное управление доступом (fine-grained access control), но процесс принятия решения о доступе в ней является более сложным и влечет за собой другую известную проблему – проблему «взрыва правил», что делает анализ безопасности ИС трудным, а иногда невозможным.

С целью нивелирования недостатков и эффективного использования взаимодополняющих преимуществ моделей RBAC и ABAC Р. Куном и др. был предложен и получил наибольшее признание в научном сообществе подход к их объединению – атрибутивная модель на основе ролей [9], которая сохраняет преимущества ролевой модели в части удобства администрирования (после определения ролей и разрешений) и упрощения процесса формального анализа безопасности, предотвращая при этом «взрыв ролей» и «взрыв правил» при необходимости учета всех возможных непредвиденных обстоятельств, которые могут возникнуть в процессе обеспечения доступа пользователей к ресурсам.

Однако открытой научно-технической проблемой этой гибридной модели, равно как и моделей RBAC и ABAC по отдельности, остается невозможность их использования в «чистом» виде в КМИС, где одновременно обрабатывается информация различных уровней конфиденциальности и видов (коммерческая, служебная, государственная тай-

на), а пользователи, соответственно, имеют различные права доступа к такой информации. В таких системах предъявляются повышенные требования к обеспечению конфиденциальности информации и контролю информационных потоков [10, 11] и соблюсти их возможно только с помощью реализации дополнительно мандатного управления доступом, которое само по себе является полноценным, отдельным механизмом со своей формализацией.

В опубликованных ранее работах не было представлено формальной модели управления доступом, которая объединяла бы в себе модели RBAC, ABAC и MAC, обеспечивая выполнение трёх известных свойств безопасности по Беллу-ЛаПадуле [3] и сохраняя возможность предоставления доступа высокой степени детализации на основе атрибутов контекста. В работе [12] С. Цзинь и др. представили формальную модель $ABAC_{\alpha}$, способную выразить модели DAC, MAC и RBAC, однако речь в ней идет только об описании конфигурации модели MAC для ее реализации на базе архитектуры XACML. По сути, это все та же классическая модель мандатного управления доступом со своими ограничениями, которую авторы выразили в терминах ABAC. В статье [13] Л. Керр и Д. Алвес-Фосс представили комбинированную модель, объединяющую MAC и ABAC, для систем, где набор атрибутов и возможных значений для них заранее известен и фиксирован. Следовательно, число возможных комбинаций атрибутов относительно невелико, что делает задачу проверки безопасности алгоритмически разрешимой, однако при возникновении необходимости предоставления более детализированного доступа на основе новых атрибутов проблема «взрыва правил» остается актуальной, а наличие в одной политике разрешающих правил как мандатного, так и атрибутивного разграничения доступа, их произвольное комбинирование, делает невозможным строгое формальное обоснование безопасности политик. Также существует ряд известных работ [14–18], в которых авторы развили упомянутый ранее подход Р. Куна и др. и представили различные варианты атрибутивных моделей управления доступом на основе ролей, сосредоточившись на совершенствовании механизмов обеспечения доступности, но в них не затрагиваются вопросы предотвращения запрещённых информационных потоков при обработке в системе информации различных уровней конфиденциальности.

В связи с вышеизложенным особую актуальность приобретает задача логического управления доступом в КМИС с повышенными требованиями как к конфиденциальности, так и к доступности информации путем объединения нескольких разнородных моделей безопасности, каждая из которых имеет формальную модель, задающую строгую семантику и обеспечиваемые свойства безопасности, в единую композиционную модель. «Механическое» объединение нескольких моделей без учета специфики каждой из них и особенностей среды, в которой требуется обеспечить управление доступом, может привести к нарушению их ключевых свойств безопасности и возникновению запрещенных потоков информации в защищаемой системе [19].

Целью данной статьи является представление результатов разработки на основе методологии субъект-сущностного подхода теории информационной безопасности, а также методологии теории автоматов новой мандатной атрибутивно-ролевой модели управления доступом (MAP модель; MRABAC), использование которой позволит сохранить высокий уровень доступности путем повышения степени автоматизации и сокращения времени администрирования системы управления доступом и одновременно обеспечить конфиденциальность информации при необходимости предоставления детализированного доступа на основе атрибутов контекста путем сохранения свойств безопасности моделей MAC и RBAC.

Структура статьи выглядит следующим образом: в разделе 1 дано общее описание разработанной модели, в разделе 2 она описана формально, в разделе 3 представлен пример реализации MAP модели. В Заключении подводятся итоги исследования и освещаются некоторые возможные направления будущей работы по исследуемой проблематике.

1. MAP модель управления доступом. Логической основой для формирования MAP модели (рис. 1) служит атрибутивная модель управления доступом на основе ролей RABAC, представленная С. Цзинем и др. в 2012 году [14], где авторы добавляют фильт-

рацию разрешений на операции с объектами на основе атрибутов с целью ограничения набора разрешений роли, доступных для каждой сессии пользователя, не изменяя базовую структуру модели RBAC. В процессе назначения прав активируется сессия s аутентифицированного пользователя u, где пользователю u назначается множество ролей R, на котором задается иерархия в виде отношения частичного порядка «≤», где вышестоящие роли наследуют разрешения нижестоящих ролей, множеству ролей R назначается множество разрешений P на операции OPS с объектами O. Далее доступное множество разрешений P ограничивается при помощи набора атрибутивных политик фильтрации разрешений PFP, содержащих наборы функций фильтрации $F_1, F_2, \ldots, F_n$ на основе конечного набора атрибутов пользователя $UATT$, конечного набора атрибутов объекта $OATT$, после чего вычисляется окончательное доступное множество разрешений P'. Внедрение PFP решает проблему «взрыва ролей» RBAC, сохраняя статические отношения между ролями и разрешениями.

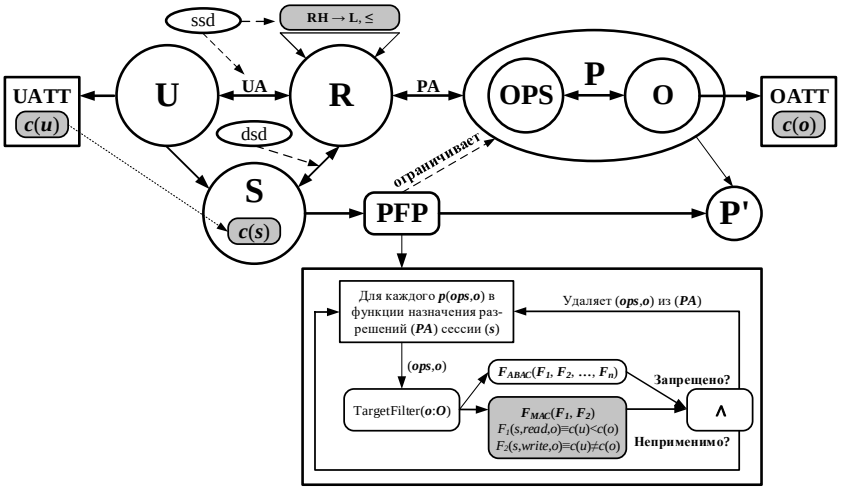

Рис. 1. Структура элементов MAP модели управления доступом

Сокращение времени администрирования системы управления доступом при ее функционировании на базе модели RABAC обеспечивается тем, что комбинация ролевых и атрибутивных политик устраняет необходимость в назначении дополнительных ролей пользователю. Атрибутивные политики покрывают множество условий, одно правило может охватывать множество обновлений ролевой модели и, следовательно, может значительно сократить административные усилия по разработке и обновлению набора ролей, которые являются главным фактором, влияющим на временные задержки при предоставлении доступа. Также, атрибутивный подход обеспечивает возможность доступа любой степени детализации с учетом меняющегося контекста.

Новым в разработанной нами модели является следующее:

- в набор атрибутов пользователя $UATT$ добавляется атрибут уровня доступа пользователя $c(u)$, в набор атрибутов объекта $OATT$ добавляется атрибут уровня конфиденциальности объекта $c(o)$, активируемой сессии s присваивается уровень доступа $c(s)$, соответствующий уровню доступа пользователя $c(u)$;
- в иерархии на множестве ролей R реализуются условия, по которым разрешения на операцию чтения наследуются, если уровень конфиденциальности объекта доступа $c(o_1)$ нижестоящей роли не превышает уровень конфиденциальности объекта доступа $c(o_2)$ вышестоящей роли, разрешения на операцию записи от нижестоящей роли к вышестоящей не наследуются, для этой цели в набор атрибутивных политик фильтрации разрешений PFP добавляется набор функций фильтрации, образующих политику F_{MAC}, представляющих собой логические выражения на основе атрибутов $c(u)$, $c(o)$ в виде запрещающих правил на операцию чтения пользователем u объекта o, принадлежащего

множеству объектов O, если уровень конфиденциальности объекта $c(o)$ больше уровня доступа пользователя $c(u)$, запрещающих правил на операцию записи пользователем u в объект o, принадлежащий множеству объектов O, если уровень конфиденциальности объекта $c(o)$ не равен уровню доступа пользователя $c(u)$.

Таким образом реализуется решетка уровней конфиденциальности L в защищаемой системе, из множества разрешений P динамически исключаются разрешения, нарушающие принципы мандатного разграничения доступа, обеспечивается конфиденциальность информации и предотвращаются информационные потоки от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности.

Стоит отметить, что в MAP модели мы используем строгое мандатное управление доступом, как наиболее безопасный вариант модели Белла-ЛаПадулы.

Определение 1. Доступ пользователя к объекту в рамках активируемой сессии доступа является безопасным для строгого мандатного управления доступом, когда выполняется одно из условий:

- разрешена операция чтения и $c(u) \geq c(o)$ (*ss*-свойство);
- разрешена операция записи в объект o и $c(u) = c(o)$, и, если разрешена операция чтения объекта o', то $c(o) = c(o')$ (строгое *-свойство) [18].

Обеспечение конфиденциальности информации и предотвращение запрещенных информационных потоков в защищаемой системе при реализации MAP модели осуществляется путем последовательного выполнения подсистемой авторизации системы управления доступом, архитектура которой определяется стандартом XACML, операций по обработке поступающих запросов пользователей на доступ к объектам (ресурсам) и вычислению итогового решения о доступе на основе набора атрибутивных политик фильтрации разрешений *PFP*, содержащего набор функций фильтрации F_{MAC} строго в виде запрещающих правил, результаты которых имеют приоритет над разрешениями, назначенными ролям.

Приоритет запрещающих решений набора функций фильтрации F_{MAC} над разрешениями ролей обусловлен применением известного алгоритма комбинирования политик Deny-overrides (рис. 2), при котором в случае, если какое-либо решение оценивается как запрещающее или ни одно решение не оценивается как разрешающее (нет соответствующей политики, соответствующей контексту запроса), результатом является запрет на доступ, если же все решения оцениваются как разрешающие, результатом является разрешение.

Так, конфиденциальность информации и контроль информационных потоков обеспечиваются тем, что даже если роли r будут назначены максимально «широкие» разрешения P (в соответствии с моделью RBAC) и при этом будут учтены все возможные атрибуты контекста *UATT, OATT* в части детализированного доступа (в соответствии с моделью ABAC), фактически пользователь сможет воспользоваться только теми разрешениями из множества P', где выполнены условия: $c(u) \geq c(o)$ для операции чтения и $c(u) = c(o)$ для операции записи.

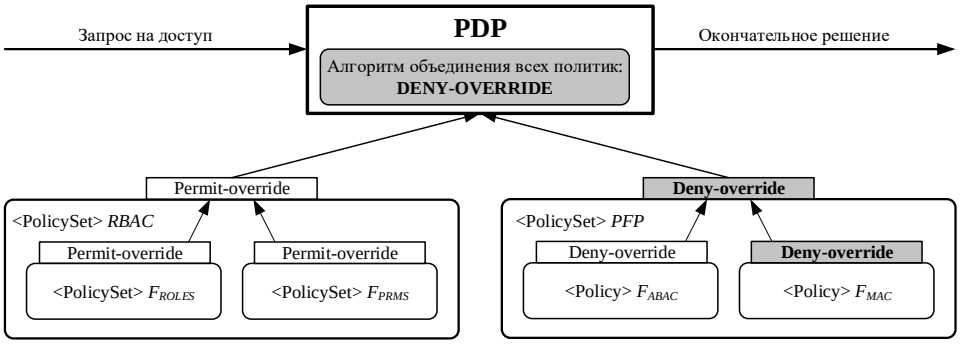

Рис. 2. Схема комбинирования политик безопасности в MAP модели

Важно обратить внимание на то, как в представленной модели обеспечивается выполнение ключевого свойства безопасности модели RBAC, состоящего в том, что для получения доступа к чему-либо субъект должен иметь привязанную роль, имеющую права на этот доступ [20].

Важной частью MAP модели является независимый компонент ABAC, реализованный в виде *PFP*, что обуславливает необходимость предотвращения проблемы «взрыва правил» в процессе предоставления разрешений на доступ. Политика RBAC и политики набора *PFP* возвращают разные результаты при обработке запросов на доступ. Тогда как RBAC возвращает только положительные решения *Permit* (разрешено), *PFP* используется только для сокращения этих разрешений, соответственно, для сохранения свойства безопасности RBAC, не должно быть функций фильтрации, которые оцениваются как разрешающие. Как и в модели RABAC, это достигается комбинированием всех политик по алгоритму Deny-overrides.

2. Математическое описание модели. Для формального описания MAP модели мы используем следующие множества и функции:

U – множество пользователей;

S – множество сессий доступа;

O – множество объектов доступа;

R – множество ролей;

$RH \subseteq R \times R$ – иерархия ролей;

$Cl_{RH}(X)$ – транзитивно-рефлексивное замыкание множества ролей X по RH;

P – множество разрешений;

P' – множество разрешений после фильтрации;

$OPS = \{read, write\}$ – множество операций;

$user: S \to U$, функция принадлежности сессии пользователю;

$roles: S \to 2^R$, функция активации ролей в сессии;

$UA: U \to 2^R$, функция назначения ролей;

$PA: R \to 2^P$, функция назначения разрешений;

$UA \subseteq U \times R$; $PA \subseteq R \times P$; $P \in 2^{(OPS \times O)}$; $P' \subseteq P$;

$UATT$ – множество атрибутов пользователя;

$OATT$ – множество атрибутов объекта;

$EATT$ – множество атрибутов среды;

PP – политики фильтрации;

$L, \leq$ – решетка уровней конфиденциальности;

$f_{ul}: U \to L$ – функция уровней доступа пользователей;

$f_{ol}: O \to L$ – функция уровней конфиденциальности объектов;

$f_{sl}: S \to L$ – функция уровней доступа активируемых сессий;

$\forall s \in S: f_{sl}(s) \leq f_{ul}(user(s))$;

$c(u) \in UATT$; $c(o) \in OATT$ – атрибуты конфиденциальности;

$\forall att \in UATT \cup OATT \; \exists Range(att)$ – диапазон атрибута, конечный набор атомарных значений;

$F_{attType}: UATT \cup OATT \to \{set, atomic\}$ – функция, задающая тип атрибута (набор или атомарный);

$F_{filter\_p}: P \to 2^{PP}$, функция фильтрации разрешений, отображение P на множество политик фильтрации разрешений PP;

$$\forall pp \in PP, pp: U \times R \times P \times 2^{UATT} \times 2^{OATT} \times 2^{EATT} \to \{t, f\};$$

$$P' = \{\forall p \in P \mid \forall pp \in PP: pp(u, r, p, UATT, OATT, EATT) \neq deny\}.$$

Модель формально выражается как детерминированный конечный автомат [21] в виде набора $V = (\Sigma, Q, \varphi, q_0, Q_F)$, где Σ и Q – входной алфавит и множество состояний, $q_0 \in Q$ – начальное состояние, $Q_F \subset Q$ – множество конечных состояний, $\varphi: Q \times \Sigma \to Q$ – функция переходов. $\Sigma = \{id, r, p, uatt, oatt, eatt, c(u), c(o)\}$, где $id, c(u), uatt \in UATT$; $c(o), oatt \in OATT$; $eatt \in EATT$, при этом $id, c(u), c(o)$ – обязательные символы каждого входного слова языка $L \subseteq \Sigma^*$, остальные символы – атрибуты контекста. В Q_F входят только два состояния – доступ разрешен (q_t), доступ запрещен (q_f).

Переходы из состояния в состояние (рис. 3) можно описать следующим образом:

$\varphi(q_0, id(u)) = q_1$ – начало сессии, извлечение R на основе id пользователя;

$\varphi(q_1, R) = q_2$ – извлечение разрешений P из набора R;

$\varphi(q_2, \{P, UATT, OATT, EATT, c(u), c(o)\}) = q_3$ – получение P' путем фильтрации на основе атрибутов безопасности и атрибутов контекста;

$\varphi(q_3, P') = q_t$ – доступ разрешен;

$\varphi(q_3, \varepsilon) = q_f$ – отказ в доступе если $P' = \varnothing$.

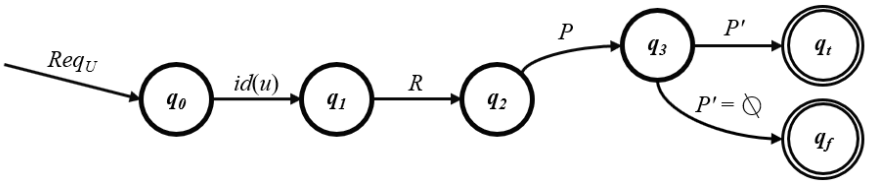

Рис. 3. Диаграмма переходов абстрактного автомата MAP модели

Доказательство безопасности. В рамках MAP модели условия безопасности формулируются через невозможность нарушения требований мандатного управления доступом (запрет на создание явных запрещенных информационных потоков «сверху-вниз»). В отличие от известной модели мандатного ролевого управления доступом [22] выполнение заданных в определении 1 свойств безопасности достигается тем, что исключение запрещенных операций происходит не статически (путем разделения ролей «на чтение» *x_read* и «на запись» *x_write*), а динамически, с помощью атрибутивной политики F_{MAC}, которая накладывает дополнительные ограничения на процесс активации сессии s и исключает из ролей (имеющих права и на чтение, и запись) ту или иную операцию согласно правилам политики.

Определение 2. Модель атрибутивного управления доступом на основе ролей соответствует требованиям строгого мандатного управления доступом, когда иерархия на множестве ролей RH в виде отношения частичного порядка «≤» соответствует требованиям, по которым разрешения на операцию чтения наследуются, если уровень конфиденциальности объекта доступа $c(o_1)$ нижестоящей роли не превышает уровень конфиденциальности объекта доступа $c(o_2)$ вышестоящей роли, разрешения на операцию записи от нижестоящей роли к вышестоящей не наследуются и выполняются ограничения:

- ограничение функции активации ролей в сессии *roles*: для каждой сессии $s \in S$ выполняется условие $roles(s) \subseteq Cl_{RH}(\{r | (user(s), r) \in UA\})$;
- ограничение функции назначения разрешений ролям PA:

а) назначение разрешений ролевыми политиками:

$$allow_{RBAC}(u, o, ops) :\Leftrightarrow \exists s \in S: user(s) = u \wedge \exists r \in roles(s): (r, (o, ops)) \in PA;$$

б) успешное прохождение разрешениями этапов фильтрации *PFP* (политика F_{MAC}):

$$F_{MAC}(u, o, read) :\Leftrightarrow c(u) \geq c(o);$$

$$F_{MAC}(u, o, write) :\Leftrightarrow c(u) = c(o);$$

в) получение разрешения пользователем (Deny-overrides):

$$permit(u, o, ops) :\Leftrightarrow allow_{RBAC}(u, o, ops) \wedge F_{MAC}(u, o, ops).$$

В рамках модели дадим определение информационного потока.

Определение 3. Информационный поток от объекта $o \in O$ к объекту $o' \in O$ существует тогда и только тогда, когда существуют роли $r, r' \in R$, сессия s такие, что разрешение на чтение объекта $(o, read) \in PA(r)$, разрешение на запись объекта $(o', write) \in PA(r')$, фактически разрешенные операции пользователя $u = user(s)$: $permit(u, o, read) \wedge permit(u, o', write)$ и роли r, r' активированы в одной сессии s.

Обоснуем, что в предлагаемой модели, соответствующей требованиям строгого мандатного управления доступом, невозможна реализация запрещенных информационных потоков от объектов с высоким уровнем конфиденциальности к объектам с низким уровнем конфиденциальности.

Теорема 1. Если модель атрибутивного управления доступом на основе ролей соответствует требованиям строгого мандатного управления доступом, то в ней для любых объектов $o, o' \in O$ таких, что $c(o) > c(o')$, невозможно возникновение информационного потока от o к o'.

Доказательство. От противного. Пусть существуют объекты $o, o' \in O$ такие, что $c(o) > c(o')$ и возможно возникновение информационного потока от o к o'. По определению 3 существуют роли $r, r' \in R$, сессия s такие, что разрешение на чтение объекта $(o, read) \in PA(r)$, разрешение на запись объекта $(o', write) \in PA(r')$ и роли r, r' активированы в одной сессии s. Следовательно, атрибутивной политикой фильтрации F_{MAC} реализуются требования строгого мандатного управления доступом и выполняются условия: уровень доступа пользователя $c(u) \geq c(o)$ и одновременно $c(u) = c(o')$. Отсюда $c(o) \leq c(o')$.

Противоречие. Если $c(o) > c(o')$, то ни один пользователь в рамках одной сессии не может одновременно получить разрешение на чтение o и запись o'. Теорема доказана.

3. Реализация модели. Закономерным итогом любого исследования в области технических наук является практическое внедрение его результатов. Для демонстрации возможности такого внедрения в данном разделе мы сосредоточились на том, как MAP модель может быть реализована на базе архитектуры XACML. В частности, мы приводим пример реализации, по аналогии с тем, как это сделано в работе [14] и предлагаем вариант кода политики безопасности, порождаемой моделью.

Пример. Защищаемой системой в рамках примера может считаться любая государственная или частная КМИС, имеющая в своем составе множество разнородных информационных систем, где одновременно обрабатывается информация различных уровней конфиденциальности и, ввиду особенностей функционирования, для обеспечения гибкого, детализированного доступа пользователей к ресурсам с учетом множества факторов (контекста) реализуется эталонная архитектура управления доступом ABAC/XACML в соответствии со стандартами [7, 8].

Сценарий доступа. Во множестве информационных систем, входящих в КМИС, реализуется множество совместных проектов, требующих информационного взаимодействия пользователей. Каждый пользователь и объект в КМИС имеют соответствующие метки безопасности в виде атрибутов уровня доступа, атрибутов уровня конфиденциальности соответственно. Для каждой из информационных систем существует отдельная роль с правами на доступ строго к объектам этой системы, а также существует единая гостевая роль для информационных систем, имеющая права на доступ строго к объектам в рамках совместных проектов (единая роль – результат решения проблемы «взрыва ролей» с помощью модели RABAC, в классическом RBAC потребовалось бы создание и назначение отдельных ролей под каждый проект и под каждое новое условие). Пользователю должен быть предоставлен доступ к объекту в рамках совместного проекта, реализуемого в сторонней информационной системе из состава КМИС, с учетом контекста (путем использования всевозможных атрибутивных политик, например: доступ к объекту в рамках совместного проекта может быть одобрен только в рабочее время; запрос должен быть сделан с любого устройства, входящего в состав КМИС; пользователю могут быть разрешены операции только с объектами, относящимся к проектам, в которых он участвует и др.) и необходимости соблюдения требований строгого мандатного управления доступом.

На начальном этапе в точку соблюдения политики PEP подсистемы авторизации системы управления доступом КМИС (рис. 4) поступает запрос $Z = (id, c(u), UATT)$ аутентифицированного пользователя u на доступ к объекту o, где id – идентификатор пользователя, $c(u)$ – обязательный атрибут уровня доступа пользователя, $UATT$ – конечное множество атрибутов пользователя, сформированное в зависимости от условий ($c(u) \in UATT$, $c(o) \in OATT$, но для наглядности примера выделяются в отдельные атрибуты, поскольку являются обязательными элементами каждого запроса на доступ независимо от контекста).

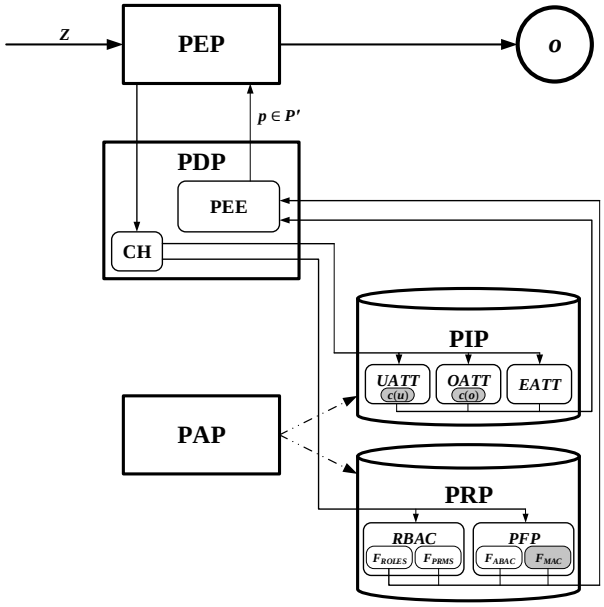

Рис. 4. Реализация MAP модели в подсистеме авторизации системы управления доступом, архитектура которой определяется стандартом XACML

PEP перенаправляет запрос Z в точку принятия решения по политике PDP, где модуль обработки контекста CH преобразует запрос Z формата соответствующей операционной среды в запрос формата доступа XACML, на основании которого PDP извлекает: из точки информирования по политике PIP, которая является логическим хранилищем атрибутов пользователей, объектов и среды, соответствующие значения атрибутов; из точки извлечения политик PRP, которая является логическим хранилищем политик безопасности, соответствующие политики и наборы политик, алгоритмы их комбинирования.

Далее, на основе полученных атрибутов пользователя, объекта и среды (*EATT*), политик, наборов политик и алгоритмов их комбинирования в модуле оценки политик PEE точки принятия решения по политике PDP происходит вычисление итогового решения о доступе путем выполнения следующих операций:

1) используя политику F_{ROLES} набора политик назначения ролей и разрешений (политика RBAC), пользователю u на основе его id назначается набор ролей R, $u \rightarrow R$;

2) используя политику F_{PRMS} набора политик назначения ролей и разрешений (политика RBAC), ролям R назначается множество разрешений P, $R \rightarrow P$;

3) используя набор политик *PFP* (политика ABAC), из множества разрешений P удаляются разрешения, нарушающие правила, сформированные на основе функций фильтрации F_1, F_2, …, F_n соответствующих политик и значений атрибутов *UATT*, *OATT* и *EATT* в соответствии с контекстом запроса;

4) используя политику F_{MAC} (политика MAC), из множества разрешений P удаляются разрешения, нарушающие правила, согласно которым для операции чтения должно выполняться условие $c(u) \geq c(o)$, для операции записи должно выполняться условие $c(u) = c(o)$, и, таким образом, вычисляется окончательное доступное множество разрешений P', $P \rightarrow P'$.

Далее решение о доступе (либо об отказе в доступе) направляется из PDP обратно в PEP с целью его исполнения: при отрицательном решении PEP блокирует запрос на доступ Z, при положительном решении обеспечивает выполнение операции с объектом.

Благодаря реализации представленной модели на базе архитектуры XACML, в защищаемой системе обеспечивается выполнение *ss*-свойства и строгого *-свойства политикой F_{MAC} одновременно, путем динамической проверки точкой принятия решения по политике (PDP) каждого перехода между состояниями в защищаемой системе в момент

запроса на этот переход, неизбежно поступающего в точку соблюдения политики (PEP). Так как атрибут уровня конфиденциальности объекта $c(o)$ в разработанной модели является обязательным для каждого объекта защищаемой системы, функции фильтрации политики F_{MAC} будут вызываться для проверки *каждой* операции из P. Таким образом, в окончательное доступное множество разрешений P' войдут только те разрешения, которые соответствуют принципам мандатного разграничения доступа.

Профиль XACML. Учитывая все вышесказанное, мы реализовали набор политик мандатного атрибутивно-ролевого управления доступом в коде XACML 3.0. В настоящий момент этот набор политик прошел процедуру государственной регистрации в виде программы для ЭВМ, Роспатентом выдано соответствующее свидетельство [23].

Заключение. В этой работе мы развили подход RABAC, предложив новую мандатную атрибутивно-ролевую модель управления доступом. На основе анализа открытых источников, это первая модель, объединяющая механизмы MAC, RBAC и ABAC в единую композицию с сохранением их преимуществ. Мировую новизну нашего решения также подтверждает получение патента на изобретение Российской Федерации [24].

Результаты исследования имеют логико-семантический и формальный характер и ориентированы, прежде всего, на подтверждение свойств безопасности модели, которое открывает путь к более широкому внедрению систем управления доступом на основе атрибутов. Использование модели позволит оперативно управлять политиками безопасности при необходимости предоставления детализированного доступа и одновременно обеспечить контроль информационных потоков в защищаемой системе при обработке в ней информации различных уровней конфиденциальности. По нашему мнению, применение модели может быть особенно востребовано в КМИС с высокими требованиями к безопасности, разворачиваемых в средах виртуализации (облако ресурсов и виртуальных машин).

Дальнейшая задача исследования заключается в совершенствовании разработанной модели как в части обеспечения конфиденциальности, так и в части повышения доступности информации, как ключевых качеств функционирования системы управления доступом, и дополнении ее профиля XACML. Также важным направлением будущей работы является полное формализованное (машиночитаемое) описание MAP модели с помощью формальных методов, позволяющих строить абстрактные автоматные модели, а также ее верификация.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Богаченко Н.Ф.* Анализ проблем управления разграничением доступа в крупномасштабных информационных системах // Математические структуры и моделирование. – 2018. – № 2 (46). – С. 135-152. – DOI: 10.25513/2222-8772.2018.2.135-152. – EDN: UZQFKY.
2. *Harrison M., Ruzzo W., Ullman J.* Protection in operating systems // Communication of ACM. – 1976. – 19 (8). – P. 461-471. – DOI: 10.1145/360303.360333.
3. *Bell D.E., LaPadula L.J.* Secure Computer Systems: Mathematical Foundations // MITRE. – 1973. – Technical Report 2547, Vol. I. – P. 33.
4. *Sandhu R., Ferraiolo D., Kuhn R.* The NIST model for role-based access control: towards a unified standard // Proceedings of the Fifth ACM Workshop on Role-Based Access Control (RBAC '00). – ACM, Berlin, 2000. – P. 47-63. – DOI: 10.1145/344287.344301.
5. *Девянин П.Н.* Ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux // Прикладная дискретная математика. – 2012. – № 1 (15). – С. 69-90. – EDN: OXBJYD.
6. Патент РФ 2525481, МПК G06F 21/62. Способ обеспечения безопасности информационных потоков в защищенных информационных системах с мандатным и ролевым управлением доступом / П.Н. Девянин. – Заявка 2012146550/08, заявлено 01.11.2012, опубликовано 20.08.2014.
7. *Ferraiolo D., Chandramouli R., Hu V., Kuhn R.* A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications. – NIST.SP.800-178. – Gaithersburg, MD, 2016. – 68 p.
8. ГОСТ Р 59383-2021. Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом. – М.: Стандартинформ, 2021. – 35 с.
9. *Kuhn D.R., Coyne E.J., Weil T.R.* Adding Attributes to Role-Based Access Control // IEEE Computer. – 2010. – 43 (6). – P. 79-81. – DOI: 10.1109/MC.2010.155.

10. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: утв. решением председателя ГТК при Президенте РФ от 30.03.1992. – ФСТЭК России, 1992. – 25 с.
11. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: утв. Приказом ФСТЭК России от 11.02.2013 № 17. – ФСТЭК России, 2013. – 42 с.
12. *Jin X., Krishnan R., Sandhu R.* A unified attribute-based access control model covering DAC, MAC and RBAC // Data and Applications Security and Privacy XXVI (DBSec 2012). Lecture Notes in Computer Science. – Vol. 7371. – Springer, Berlin, Heidelberg, 2012. – P. 41-55. – DOI: 10.1007/978-3-642-31540-4_4.
13. *Kerr L., Alves-Foss J.* Combining mandatory and attribute-based access control // 49th Hawaii International Conference on System Sciences (HICSS). – IEEE, Koloa, HI, 2016. – P. 2616-2623. – DOI: 10.1109/HICSS.2016.328.
14. *Jin X., Krishnan R., Sandhu R.* RABAC: role-centric attribute-based access control // Computer Network Security (MMM-ACNS 2012). Lecture Notes in Computer Science. – Vol. 7531. – Springer, Berlin, Heidelberg, 2012. – P. 84-96. – DOI: 10.1007/978-3-642-33704-8_8.
15. *Rajpoot Q.M., Jensen C.D., Krishnan R.* Attributes Enhanced Role-Based Access Control Model // Proceedings of the 12th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'15). – Springer, Cham, 2015. – P. 3-17. – DOI: 10.1007/978-3-319-22906-5_1.
16. *Qi H., Di X., Li J.* Formal definition and analysis of access control model based on role and attribute // Journal of information security and applications. – 2018. – Vol. 43. – P. 53-60. – DOI: 10.1016/j.jisa.2018.09.001.
17. *Houhou O., Bitam S., Hamida A.* HYARBAC: a new hybrid access control model for cloud computing // International Journal of Computing and Digital Systems. – 2024. – Vol. 15, No. 1. – P. 403-414. – DOI: 10.12785/ijcds/150131.
18. *Shahraki A.S., Rudolph C., Alavizadeh H. et al*. Securing cross-domain data access with decentralized attribute-based access control // Ad Hoc Networks. – 2025. – Vol. 173. – 103807. – P. 1-15. – DOI: 10.1016/j.adhoc.2025.103807.
19. *Девянин П.Н., Кулямин В.В., Петренко А.К. [и др.].* Интеграция мандатного и ролевого управления доступом и мандатного контроля целостности в верифицированной иерархической модели безопасности операционной системы // Тр. ИСП РАН. – 2020. – Т. 32, № 1. – С. 7-26. – DOI: 10.15514/ISPRAS-2020-32(1)-1. – EDN: WSVFME.
20. *Девянин П.Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. – 3-е изд. – М.: Горячая линия – Телеком, 2024. – 352 с.
21. *Хопкрофт Д.Э., Мотвани Р., Ульман Д.* Введение в теорию автоматов, языков и вычислений. – М.: Издательский дом Вильямс, 2008. – 528 с.
22. *Sandhu R.* Role-based access control // Advances in Computers. – 1998. – 46. – P. 237-286. – DOI: 10.1016/S0065-2458(08)60206-5.
23. Свидетельство о государственной регистрации программы для ЭВМ № 2025687752, Российская Федерация. Программный модуль набора политик мандатного атрибутивно-ролевого управления доступом в крупномасштабных информационных системах / Д.О. Ларин. – Заявлено 09.10.2025, опубликовано 15.10.2025. – EDN: RNTBUM.
24. Патент на изобретение РФ 2847174, МПК G06F 21/62. Способ обеспечения конфиденциальности информации в гетерогенных крупномасштабных распределенных информационных системах с атрибутивным управлением доступом / Д.О. Ларин, Р.И. Захарченко, С.А. Диченко. – Заявка 2025112755, заявлено 12.05.2025, опубликовано 29.09.2025. – EDN: EFYGAL.

REFERENCES

1. *Bogachenko N.F.* Analiz problem upravleniya razgranicheniem dostupa v krupnomasshtabnykh informatsionnykh sistemakh [Analysis of problems of access control management in large-scale information systems], *Matematicheskie struktury i modelirovanie* [Mathematical Structures and Modeling], 2018, No. 2 (46), pp. 135-152. DOI: 10.25513/2222-8772.2018.2.135-152. EDN: UZQFKY.
2. *Harrison M., Ruzzo W., Ullman J.* Protection in operating systems, *Communication of ACM*, 1976, 19 (8), pp. 461-471. DOI: 10.1145/360303.360333.
3. *Bell D.E., LaPadula L.J.* Secure Computer Systems: Mathematical Foundations, *MITRE,* 1973. Technical Report 2547, Vol. I, pp. 33.
4. *Sandhu R., Ferraiolo D., Kuhn R.* The NIST model for role-based access control: towards a unified standard, *Proceedings of the Fifth ACM Workshop on Role-Based Access Control (RBAC '00)*. ACM, Berlin, 2000, pp. 47-63. DOI: 10.1145/344287.344301.

5. *Devyanin P.N.* Rolevaya DP-model' upravleniya dostupom i informatsionnymi potokami v operatsionnykh sistemakh semeystva Linux [Role-based DP-model for managing access and information flows in Linux operating systems], *Prikladnaya diskretnaya matematika* [Applied Discrete Mathematics], 2012, No. 1 (15), pp. 69-90. EDN: OXBJYD.
6. *Devyanin P.N.* Patent RF 2525481, MPK G06F 21/62. Sposob obespecheniya bezopasnosti informatsionnykh potokov v zashchishchennykh informatsionnykh sistemakh s mandatnym i rolevym upravleniem dostupom [Patent RF 2525481, IPC G06F 21/62. Method of securing information flow in secure information systems with mandatory and role-based access control]. Application 2012146550/08, filed November 1, 2012, published August 20, 2014.
7. *Ferraiolo D., Chandramouli R., Hu V., Kuhn R.* A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications. NIST.SP.800-178. Gaithersburg, MD, 2016, 68 p.
8. GOST R 59383-2021. Informatsionnye tekhnologii. Metody i sredstva obespecheniya bezopasnosti. Osnovy upravleniya dostupom [GOST R 59383-2021. Information technologies. Methods and tools of ensuring security. Fundamentals of access control]. Moscow: Standartinform, 2021, 35 p.
9. *Kuhn D.R., Coyne E.J., Weil T.R.* Adding Attributes to Role-Based Access Control, *IEEE Computer*, 2010, 43 (6), pp. 79-81. DOI: 10.1109/MC.2010.155.
10. Rukovodyashchiy dokument. Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii: utv. resheniem predsedatelya GTK pri Prezidente RF ot 30.03.1992 [Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and information protection requirements: approved by the decision of the Chairman of the State Customs Committee under the President of the Russian Federation dated March 30, 1992]. FSTEK Rossii, 1992, 25 p.
11. Requirements for the protection of information that does not constitute a state secret, contained in state information systems: approved. by Order of the FSTEC of Russia dated 11.02.2013 No. 17 [Requirements for the protection of information that does not constitute a state secret contained in state information systems: approved by Order of the Federal Service for Technical and Export Control of Russia dated February 11, 2013, No. 17]. FSTEC of Russia, 2013, 42 p.
12. *Jin X., Krishnan R., Sandhu R.* A unified attribute-based access control model covering DAC, MAC and RBAC, *Data and Applications Security and Privacy XXVI (DBSec 2012). Lecture Notes in Computer Science*, Vol. 7371. Springer, Berlin, Heidelberg, 2012, pp. 41-55. DOI: 10.1007/978-3-642-31540-4_4.
13. *Kerr L., Alves-Foss J.* Combining mandatory and attribute-based access control, *49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, Koloa, HI, 2016, pp. 2616-2623. DOI: 10.1109/HICSS.2016.328.
14. *Jin X., Krishnan R., Sandhu R.* RABAC: role-centric attribute-based access control, *Computer Network Security (MMM-ACNS 2012). Lecture Notes in Computer Science*, Vol. 7531. Springer, Berlin, Heidelberg, 2012, pp. 84-96. DOI: 10.1007/978-3-642-33704-8_8.
15. *Rajpoot Q.M., Jensen C.D., Krishnan R.* Attributes Enhanced Role-Based Access Control Model, *Proceedings of the 12th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'15)*. Springer, Cham, 2015, pp. 3-17. DOI: 10.1007/978-3-319-22906-5_1.
16. *Qi H., Di X., Li J.* Formal definition and analysis of access control model based on role and attribute, *Journal of information security and applications*, 2018, Vol. 43, pp. 53-60. DOI: 10.1016/j.jisa.2018.09.001.
17. *Houhou O., Bitam S., Hamida A.* HYARBAC: a new hybrid access control model for cloud computing, *International Journal of Computing and Digital Systems*, 2024, Vol. 15, No. 1, pp. 403-414. DOI: 10.12785/ijcds/150131.
18. *Shahraki A.S., Rudolph C., Alavizadeh H. et al*. Securing cross-domain data access with decentralized attribute-based access control, *Ad Hoc Networks*, 2025, Vol. 173, 103807, pp. 1-15. DOI: 10.1016/j.adhoc.2025.103807.
19. *Devyanin P.N., Kulyamin V.V., Petrenko A.K. [i dr.]*. Integratsiya mandatnogo i rolevogo upravleniya dostupom i mandatnogo kontrolya tselostnosti v verifitsirovannoy ierarkhicheskoy modeli bezopasnosti operatsionnoy sistemy [Integrating RBAC, MIC, and MLS in Verified Hierarchical Security Model for Operating System], *Tr. ISP RAN* [Proceedings of the Institute for System Programming of the RAS], 2020, Vol. 32, No. 1, pp. 7-26. DOI: 10.15514/ISPRAS-2020-32(1)-1. EDN: WSVFME.
20. *Devyanin P.N.* Modeli bezopasnosti komp'yuternykh sistem. Upravlenie dostupom i informatsionnymi potokami [Computer system security models. Access and information flow control]. 3rd ed. Moscow: Goryachaya liniya – Telekom, 2024, 352 p.

21. *Khopkroft D.E., Motvani R., Ul'man D.* Vvedenie v teoriyu avtomatov, yazykov i vychisleniy [Introduction to automata theory, languages, and computation]. Moscow: Izdatel'skiy dom Vil'yams, 2008, 528 p.
22. *Sandhu R.* Role-based access control, *Advances in Computers*, 1998, 46, pp. 237-286. DOI: 10.1016/S0065-2458(08)60206-5.
23. *Larin D.O.* Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2025687752, Rossiyskaya Federatsiya. Programmnyy modul' nabora politik mandatnogo atributivno-rolevogo upravleniya dostupom v krupnomasshtabnykh informatsionnykh sistemakh [Certificate of state registration of a computer program No. 2025687752 RF. A software module for a set of mandatory role-centric attribute-based access control policies in large-scale information systems]. Announced October 9, 2025, published October 15, 2025. EDN: RNTBUM.
24. *Larin D.O., Zakharchenko R.I., Dichenko S.A.* Patent na izobretenie RF 2847174, MPK G06F 21/62. Sposob obespecheniya konfidentsial'nosti informatsii v geterogennykh krupnomasshtabnykh raspredelennykh informatsionnykh sistemakh s atributivnym upravleniem dostupom [Patent RF 2847174, IPC G06F 21/62. Method for ensuring information confidentiality in heterogeneous large-scale distributed information systems with attribute-based access control]. Application 2025112755, submitted May 12, 2025, published September 29, 2025. EDN: EFYGAL.

Ларин Даниил Олегович – Краснодарское высшее военное училище им. генерала армии С.М. Штеменко; e-mail: jwlll@bk.ru; г. Краснодар, Россия; тел.: +79999830810; адъюнкт; ORCID 0009-0006-4943-0273; WoS ResearcherID LOS-0856-2024.

Захарченко Роман Иванович – Краснодарское высшее военное училище им. генерала армии С.М. Штеменко; e-mail: romanzakharchenko@yandex.ru; г. Краснодар, Россия; тел.: +78612581030; д.т.н.; доцент; начальник кафедры.

Диченко Сергей Александрович – Краснодарское высшее военное училище им. генерала армии С.М. Штеменко; e-mail: dichenko.sa@yandex.ru; г. Краснодар, Россия; тел.: +78612683805; д.т.н.; начальник управления научно-исследовательского центра.

Larin Daniel Olegovich – General of the Army S.M. Shtemenko Krasnodar Higher Military School; e-mail: jwlll@bk.ru; Krasnodar, Russia; phone: +79999830810; Graduate Student (PhD); ORCID 0009-0006-4943-0273; WoS ResearcherID LOS-0856-2024.

Zaharchenko Roman Ivanovich – General of the Army S.M. Shtemenko Krasnodar Higher Military School; e-mail: romanzakharchenko@yandex.ru; Krasnodar, Russia; phone: +78612581030; dr. eng. of sc.; associate professor; head of Department.

Dichenko Sergej Aleksandrovich – General of the Army S.M. Shtemenko Krasnodar Higher Military School; e-mail: dichenko.sa@yandex.ru; Krasnodar, Russia; phone: +78612683805; dr. eng. of sc.; head of the Research Center Directorate.