СРАВНЕНИЕ ЭФФЕКТИВНОСТИ ГИБРИДНОГО ПОДХОДА ЗАЩИТЫ ДАННЫХ С КЛАССИЧЕСКИМИ МОДЕЛЯМИ УПРАВЛЕНИЯ ДОСТУПОМ (МАНДАТНОЕ/ДИСКРЕЦИОННОЕ УПРАВЛЕНИЕ)

Насырова Динара Тагировна
студент группы 304-25
направления «Компьютерные сети и их программное обеспечение»
Ташкентского университета
информационных технологий имени Мухаммада аль-Хорезми
Решитов Эльдар Серверович
ассистент
кафедры «Системное прикладное программирование»
Ташкентского университета
информационных технологий имени Мухаммада аль-Хорезми

Аннотация. Данная статья, выполненная в формате научно-исследовательской работы, посвящена сравнительному анализу эффективности гибридных подходов к защите данных и традиционных классических моделей управления доступом – мандатного (MAC) и дискреционного (DAC). В условиях экспоненциального роста объемов данных, усложнения киберугроз и перехода к гибридным рабочим средам, вопрос обеспечения адекватного, гибкого и надежного управления доступом приобретает критическую актуальность. Традиционные модели, обладая своими сильными сторонами (строгость MAC, простота DAC), часто оказываются недостаточными для удовлетворения современных требований к безопасности, масштабируемости и управляемости. Работа исследует преимущества и недостатки каждого подхода, обосновывая необходимость и потенциал гибридных решений как наиболее оптимального ответа на текущие вызовы информационной безопасности.

Ключевые слова: Управление доступом (Access Control), Гибридный подход (Hybrid Approach), Мандатное управление (MAC), Дискреционное управление (DAC), Информационная безопасность, Защита данных.

ВСТУПЛЕНИЕ

В современном цифровом мире информация является одним из наиболее ценных активов, а ее защита – первостепенной задачей для любой организации. Основным механизмом обеспечения конфиденциальности, целостности и доступности данных служит управление доступом (Access Control). Исторически сложились две основные, фундаментальные модели разграничения доступа: дискреционное (DAC) и мандатное (MAC). DAC, основанное на праве владельца объекта назначать разрешения, является гибким, но подвержено риску несанкционированной передачи прав. MAC, основанное на метках безопасности и строгой иерархии, обеспечивает высокий уровень защиты, но отличается жесткостью и сложностью администрирования.

Однако, развитие облачных технологий, мобильных устройств, концепции гибридной работы и Нулевого доверия (Zero Trust) привело к тому, что ни одна из классических моделей в чистом виде не может в полной мере обеспечить требуемый уровень безопасности и гибкости в динамично меняющихся условиях. Это обусловило появление и активное развитие гибридных подходов (например, сочетание элементов MAC и DAC, или интеграция с ролевым (RBAC) и контекстно-зависимым (ABAC) управлением).

Цель данной статьи — провести сравнительный анализ эффективности гибридного подхода к защите данных с классическими моделями DAC и MAC, определить ключевые преимущества и недостатки каждого решения и обосновать целесообразность использования гибридных систем в современных информационных средах.

СРАВНЕНИЕ МОДЕЛЕЙ УПРАВЛЕНИЯ ДОСТУПОМ

Таблица 1

Классические модели управления доступом

Модель	Дискреционное управление (DAC)	Мандатное управление (MAC)
Основной принцип	Владелец объекта определяет права доступа для других субъектов (пользователей/групп).	Доступ определяется сравнением меток безопасности (уровней допуска субъекта и уровня конфиденциальности объекта).
Ключевая характеристика	Гибкость, простота реализации в невысокозащищенных системах.	Строгое соблюдение политики безопасности, централизованный контроль.
Преимущества	Легкость администрирования, высокий контроль пользователя над своими объектами.	Высочайший уровень защиты конфиденциальной информации (гостайна, военная сфера).
Недостатки	Неуправляемое распространение прав доступа, уязвимость к	Крайняя негибкость, сложность администрирования,

	вредоносному ПО, действующему от имени владельца.	высокие накладные расходы.

Гибридный подход в управлении доступом представляет собой комбинацию элементов различных моделей, направленную на минимизацию их недостатков и объединение преимуществ. Наиболее распространенные гибридные системы сочетают:

- **MAC/DAC:** Применяется в системах с разным уровнем конфиденциальности данных. Например, для высокочувствительной информации используется MAC, а для менее критичных данных – DAC или RBAC.
- **RBAC/ABAC:** Ролевое управление (RBAC) обеспечивает упрощенное администрирование, назначая права ролям. Атрибутное управление (ABAC) добавляет контекст (время, местоположение, состояние устройства), что критически важно для современных гибридных и удаленных сред.

Эффективность управления доступом оценивается по следующим критериям: Безопасность (строгость политики), Гибкость, Масштабируемость и Управляемость (Администрирование).

Таблица 2

Сравнение эффективности

Критерий	**MAC**	**DAC**	**Гибридный подход (RBAC + ABAC/MAC)**
Безопасность	Высокая/Критическая (Строгая политика)	Низкая/ Средняя (Риск несанкциониро	Оптимальная (Сочетание

		ванной передачи)	строгости и контекста)
Гибкость	Низкая (Сложно менять правила)	Высокая (Права устанавливаются владельцем)	Высокая (Настраиваемые политики на основе ролей и атрибутов)
Масштабируемость	Низкая/Средняя (Сложность при росте пользователей/объектов)	Средняя/Низкая (Проблема управления множеством прав)	Высокая (Управление через роли и политики)
Управляемость	Низкая (Высокие накладные расходы)	Средняя (Зависит от числа владельцев)	Высокая (Централизованное управление политиками)

Гибридные решения, интегрирующие, например, ABAC с RBAC, позволяют принимать решения о доступе не только на основе личности или роли, но и на основе контекста (например, доступ разрешен только с корпоративного устройства, из определенной географической зоны, в рабочее время). Такая комбинация обеспечивает динамическое, контекстно-зависимое управление, что является ключевым требованием для концепции "Нулевого доверия" (Zero Trust), в которой "не доверяют никому и ничему по умолчанию".

ВЫВОД

Классические модели MAC и DAC заложили основу для систем управления доступом. MAC остается незаменимым в системах с критическими требованиями к защите, где приоритет отдается строгости над гибкостью. DAC по-прежнему используется в простых средах, где важна самостоятельность пользователей.

Однако, для современных, сложных, распределенных информационных систем, характеризующихся гибридными рабочими средами и разнородностью данных, чистые классические модели показывают свою недостаточную эффективность.

Гибридный подход доказал свою эффективность, предлагая баланс между строгостью безопасности и операционной гибкостью. Комбинирование сильных сторон различных моделей (например, MAC для критических данных, RBAC для ролевых полномочий и ABAC для контекста) позволяет создать систему управления доступом, которая адаптивна к меняющимся угрозам, масштабируема и удобна в администрировании. Именно гибридные модели, основанные на контексте и атрибутах, являются наиболее перспективным направлением развития в области управления доступом и соответствуют современным стандартам информационной безопасности, таким как Zero Trust.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Yan Cao, Changbo Ke, Dajuan Fan, Yuan Ping, Quanxin Yang, MengKe Yao, State-aware access control for cyber-physical-social space: Model and policy security assurance, Egyptian Informatics Journal, Volume 31, 2025, 100749, ISSN 1110-8665,

2. Vinod Mahor, R. Padmavathy, Santanu Chatterjee, Hybrid blockchain enabled authenticated fine grained access control for IoMT enabled smart healthcare systems, Computers and Electrical Engineering, Volume 127, Part A, 2025, 110538, ISSN 0045-7906,

3. Sondes Baccouri, Takoua Abdellatif, BIG-ABAC: Leveraging Big Data for Adaptive, Scalable, and Context-Aware Access Control, CMES - Computer Modeling in Engineering and Sciences, Volume 143, Issue 1, 2025, Pages 1071-1093, ISSN 1526-1492

4. Aya Khaled Youssef Sayed Mohamed, Dagmar Auer, Daniel Hofer, Josef Küng, A systematic literature review of authorization and access control requirements and current state of the art for different database models, International Journal of Web Information Systems, Volume 20, Issue 1, 2023, Pages 1-23, ISSN 1744-0084

5. Sana Said, JalelEddine Hajlaoui, Mohamed Nazih Omri, New privacy-respecting access control-based approach for data placement in an Internet of Things environment, Journal of Information Security and Applications, Volume 93, 2025, 104192, ISSN 2214-2126