УДК 04 **Информационные технологии**

Акимин Олег Викторович, *студент,*
ФГБОУ ВО Донской государственный технический университет

УПРАВЛЕНИЕ ДОСТУПОМ НА ОСНОВЕ РОЛЕЙ (RBAC)

Аннотация: В эпоху цифровых технологий, когда информация является ценным активом, обеспечение безопасности и конфиденциальности данных имеет первостепенное значение. Управление доступом на основе ролей (RBAC) стало мощным и эффективным методом управления доступом к информационным системам и ресурсам. RBAC - это модель безопасности, которая предоставляет права доступа на основе четко определенных ролей, обязанностей и должностных функций в организации. В статье описывается значение контроля доступа на основе ролей, его принципы, преимущества и его роль в оптимизации информационной безопасности путем предоставления детализированного и контролируемого доступа к критически важным ресурсам.

Ключевые слова: оптимизация информационной безопасности, определение ролей, информационная безопасность.

Annotation: In the digital age, where information is a valuable asset, keeping data secure and private is paramount. Role Based Access Control (RBAC) has become a powerful and efficient method for managing access to information systems and resources. RBAC is a security model that grants access rights based on well-defined roles, responsibilities, and job functions within an organization. This essay explores the meaning of role-based access control, its principles, benefits, and its role in optimizing information security by providing granular and controlled access to critical resources.

Keywords: information security optimization, definition of roles, information security.

Понимание управления доступом на основе ролей (RBAC). RBAC - это концепция безопасности, которая упрощает контроль доступа путем назначения ролей пользователям на основе их должностных обязанностей и разрешений в организации. Каждая роль связана с определенными правами доступа, привилегиями и ограничениями, что позволяет пользователям получать доступ только к ресурсам, необходимым для выполнения их рабочих функций. Модель RBAC включает в себя три основных компонента [1]:

1. Пользователи: Пользователи представляют собой физических лиц, которые получают доступ к информационной системе. Каждому пользователю назначается одна или несколько ролей в зависимости от его должностных функций или обязанностей.

2. Роли: Роли - это предопределенные наборы прав доступа и разрешений, которые представляют конкретные должностные функции или обязанности в организации.

3. Разрешения: Разрешения - это действия или операции, которые пользователям разрешено выполнять с ресурсами, такие как чтение, запись, изменение или удаление.

Принципы управления доступом на основе ролей (RBAC)

1. Наименьшие привилегии: Принцип наименьших привилегий гарантирует, что пользователям предоставляется только минимальный уровень доступа, необходимый для выполнения их рабочих функций. Это снижает риск несанкционированного доступа и потенциальной утечки данных.

2. Разделение обязанностей: Принцип разделения обязанностей направлен на предотвращение конфликта интересов и снижение риска мошенничества или злоупотребления привилегиями. Это требует, чтобы ни один пользователь не обладал всеми необходимыми разрешениями для самостоятельного выполнения критически важной задачи.

3. Иерархия ролей: RBAC позволяет создавать иерархические роли, где роли более высокого уровня наследуют разрешения от ролей более низкого

уровня. Это упрощает назначение ролей и управление ими, оптимизируя контроль доступа [2].

Преимущества управления доступом на основе ролей (RBAC)

1. Повышенная безопасность: RBAC обеспечивает надежную систему безопасности, предоставляя доступ на основе четко определенных ролей, сводя к минимуму риск несанкционированного доступа или утечки данных.

2. Масштабируемость и эффективность: RBAC упрощает управление доступом, делая его масштабируемым и эффективным, особенно в крупных организациях с большим количеством пользователей и сложными требованиями к разрешениям.

3. Соответствие требованиям и аудит: RBAC способствует соблюдению отраслевых норм и стандартов, обеспечивая соответствие политик контроля доступа передовым практикам и конкретным нормативным требованиям.

4. Снижение административных издержек: RBAC снижает административную нагрузку, связанную с управлением разрешениями отдельных пользователей, поскольку доступ управляется с помощью ролей, а не индивидуальных назначений [3].

Роль RBAC в оптимизации информационной безопасности

1. Детализированный контроль доступа: RBAC позволяет организациям назначать детализированные права доступа пользователям на основе их ролей. Это гарантирует, что пользователи смогут получить доступ только к ресурсам, необходимым для выполнения своих рабочих функций, сводя к минимуму потенциальную поверхность атаки.

2. Снижение рисков: Придерживаясь принципа наименьших привилегий, RBAC снижает риск случайной или преднамеренной утечки данных, вызванной чрезмерными разрешениями пользователей.

3. Соответствие требованиям контроля доступа: RBAC способствует соблюдению правил и стандартов защиты данных, обеспечивая систематический подход к контролю доступа, гарантируя, что только авторизованные пользователи могут получить доступ к конфиденциальной информации.

4. Динамическое управление доступом: RBAC обеспечивает динамическое управление доступом, позволяя организациям быстро корректировать разрешения пользователей по мере изменения ролей или прихода новых сотрудников в организацию или их ухода из нее.

5. Снижение инсайдерских угроз: RBAC может помочь снизить инсайдерские угрозы, внедрив разделение обязанностей, предотвращая неограниченный доступ любого отдельного пользователя к критически важным ресурсам [4].

Вывод

Управление доступом на основе ролей (RBAC) является фундаментальным аспектом информационной безопасности, оптимизирующим управление доступом путем предоставления прав на основе четко определенных ролей и обязанностей. Придерживаясь принципов наименьших привилегий и разделения обязанностей, RBAC снижает риск несанкционированного доступа и утечки данных, повышая общую информационную безопасность. Масштабируемость и эффективность RBAC делают его ценным активом для организаций любого размера, оптимизируя процессы управления доступом и обеспечивая соответствие отраслевым нормативам. Внедрение RBAC как части комплексной стратегии безопасности позволяет организациям поддерживать строгий контроль над доступом к конфиденциальным ресурсам, защищая ценную информацию от потенциальных угроз во все более взаимосвязанном и уязвимом цифровом ландшафте.

Библиографический список:

1. AUTHENTICATION AND AUTHORIZATION OF MOBILE CLIENTS IN PUBLIC DATA NETWORKS/VENKY K., KAN Z., 2002.

2. David F. Ferraiolo Role-Based Access Control/ D. Richard Kuhn, Ramaswamy Chandramouli, 1992.

3. Application of Attribute Based Access Control Model for Industrial Control Systems, 2017.

4. Das S. POLICY ENGINEERING IN RBAC AND ABAC/Sural S., Mitra B., 2018.