ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056.5

ВЫБОР МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДОСТУПА К ДАННЫМ В ПРИЛОЖЕНИЯХ POWER APPS

Тарасов Кирилл Олегович,
Студент группы ИУК5-82Б
Калужский филиал Московского государственного технического университета имени Н.Э. Баумана
kirill.tarasov1371@gmail.com

Фадеев Вячеслав Олегович,
Студент группы ИУК5-81Б
Калужский филиал Московского государственного технического университета имени Н.Э. Баумана
fadeevvo@student.bmstu.ru

Ильичёв Владимир Юрьевич,
Кандидат технических наук, доцент
Калужский филиал Московского государственного технического университета имени Н.Э. Баумана
ilyichev.vyu@bmstu.ru

Аннотация

В данной статье проводится сравнительный анализ популярных способов ограничения прав пользователей информационной системы на платформе Power Apps. Описываются основные особенности каждого способа, а также приводятся их преимущества и недостатки. Целью данного исследования является выявление оптимальных условий применения каждого из решений.

Ключевые слова: Power Apps, RBAC, TDE, RLS, Microsoft Azure.

THE CHOICE OF DATA SECURITY MECHANISMS IN POWER APPS

Kirill O. Tarasov,
Student of group IUK5-82B
Bauman Moscow State Technical University (Kaluga Branch)
kirill.tarasov1371@gmail.com

Vyacheslav O. Fadeev,
Student of group IUK5-81B
Bauman Moscow State Technical University (Kaluga Branch)
fadeevvo@student.bmstu.ru

Vladimir Y. Ilyichev,
Ph.D, Associate Professor
Bauman Moscow State Technical University (Kaluga Branch)
ilyichev.vyu@bmstu.ru

ABSTRACT

This article provides a comparative analysis of popular ways to restrict the rights of users of an information system on the Power Apps platform. The main subtleties of each method are described, as well as their advantages and disadvantages. The purpose of this study is to identify the optimal conditions for the application of each of the solutions.

Keywords: Power Apps, RBAC, TDE, RLS, Microsoft Azure.

Power Apps — это низкокодовое решение от Microsoft, позволяющее создавать приложения для мобильных устройств и веб-платформ. Оно интегрируется с различными источниками данных, такими как SharePoint, Dynamics 365, SQL Server и другими. Однако, с увеличением сложности приложений и объемов обрабатываемых данных, возникает необходимость в обеспечении их конфиденциальности, целостности и доступности. В статье рассматриваются ключевые аспекты ограничения доступа к данным в приложениях Power Apps и предлагаются подходы к выбору данных механизмов.

1. Основные угрозы безопасности данных в Power Apps
При использовании Power Apps можно столкнуться с рядом угроз, таких как:

- Несанкционированный доступ к данным.
- Утечка информации через неправильно настроенные разрешения.
- Потеря данных из-за сбоев в работе приложения или внешних атак.
- Нарушение целостности данных вследствие некорректной обработки.

Для минимизации этих рисков необходимо использовать комплексный подход к обеспечению безопасности.

2. Механизмы обеспечения безопасности данных в PowerApps

2.1. Ролевая модель доступа (Role-Based Access Control, RBAC)
Power Apps поддерживает ролевую модель доступа, которая позволяет ограничивать доступ к данным на основе ролей пользователей. Это один из наиболее эффективных способов предотвращения несанкционированного доступа [1, 2].

Преимущества: Гибкость в настройке прав доступа, интеграция с Azure Active Directory [3].

Ограничения: Требуется тщательная настройка и регулярный аудит ролей [4].

2.2. Шифрование данных
Шифрование данных как при хранении, так и при передаче является важным механизмом защиты. Power Apps интегрируется с Azure, что позволяет использовать встроенные механизмы шифрования, такие как Azure SQL Database Transparent Data Encryption (TDE).

Преимущества: Обеспечение конфиденциальности данных даже в случае утечки.

Ограничения: Возможное увеличение нагрузки на систему при обработке больших объемов данных.

2.3. Ограничение доступа на уровне данных (Row-Level Security, RLS) RLS позволяет ограничивать доступ к строкам данных в зависимости от роли или прав пользователя. Это особенно полезно в многопользовательских средах [5, 6].

Преимущества: Тонкая настройка доступа к данным [7].

Ограничения: Сложность в реализации для сложных сценариев.

3. Рекомендации по выбору механизмов безопасности

Выбор механизмов обеспечения безопасности данных в Power Apps должен основываться на следующих факторах [8, 9]:

- Тип данных: Конфиденциальные данные требуют более строгих мер защиты, таких как шифрование и RLS.
- Масштаб приложения: Для крупных приложений с множеством пользователей рекомендуется использовать RBAC и аудит.
- Интеграция с другими системами: Важно учитывать совместимость механизмов безопасности с внешними источниками данных.
- Ресурсы организации: Некоторые механизмы, такие как шифрование и аудит, могут требовать дополнительных затрат на внедрение и поддержку.

Проведём наглядный эксперимент для сравнения RBAC и RLS:

Цель эксперимента: сравнить эффективность двух механизмов обеспечения безопасности данных в Power Apps — ролевой модели доступа (RBAC) и ограничения доступа на уровне данных (RLS) — в условиях, приближенных к реальным. Оценить, какой из механизмов лучше подходит для сценариев с необходимостью тонкого контроля доступа к данным.

Условия эксперимента

Создано тестовое приложение Power Apps, подключенное к базе данных SQL Server. В базе данных содержится таблица с конфиденциальными данными (информация о сотрудниках: имя, должность, зарплата). В приложении настроены два механизма безопасности: RBAC: Роли "Менеджер" и "Сотрудник". Менеджер имеет доступ ко всем данным, а Сотрудник — только к своим данным. RLS: Ограничение доступа на уровне строк, где каждый пользователь может видеть только свои данные.

Методика проведения эксперимента

В эксперименте участвуют два пользователя: пользователь А (Менеджер), пользователь В (Сотрудник). Для каждого механизма (RBAC и RLS) выполняются следующие шаги:

- Настройка механизма безопасности.
- Тестирование доступа пользователей к данным.
- Измерение времени отклика приложения.
- Оценка сложности настройки и поддержки.

Критерии оценки

- Эффективность: Способность механизма корректно ограничивать доступ к данным.
- Производительность: Время отклика приложения при использовании механизма.
- Этапы настройки: Время и усилия, необходимые для настройки механизма.
- Гибкость: Возможность адаптации механизма к изменяющимся требованиям.

Результаты эксперимента приведены в таблице 1.

Таблица 1 – оценка критериев

Критерий	RBAC	RLS
Эффективность	Пользователь B не может получить доступ к данным других сотрудников.	Пользователь B видит только свои данные, даже если попытается обойти ограничения.
Производительность	Время отклика: 1.2 секунды.	Время отклика: 1.8 секунды (из-за дополнительных проверок на уровне строк).
Этапы настройки	Требуется настройка ролей в Azure AD и PowerApps.	Требуется настройка политик RLS в SQL Server.
Гибкость	Легко добавлять новые роли, но сложно управлять доступом на уровне строк.	Гибкость в настройке доступа на уровне строк, но сложно масштабировать.

Анализ результатов

Эффективность

- Оба механизма успешно ограничивают доступ к данным, но RLS обеспечивает более тонкий контроль на уровне строк.
- RBAC проще в управлении, но менее гибок в сценариях, где требуется ограничение доступа к конкретным строкам данных.

Производительность

- RBAC демонстрирует лучшее время отклика, так как не требует дополнительных проверок на уровне строк.
- RLS немного замедляет работу приложения из-за необходимости проверять права доступа для каждой строки.

Этапы настройки

- RBAC проще в настройке, особенно если организация уже использует Azure AD.
- RLS требует более глубоких знаний SQL Server и больше времени для настройки.

Гибкость

- RBAC подходит для сценариев, где доступ ограничивается на уровне ролей.
- RLS более гибок в сценариях, где требуется ограничение доступа на уровне строк, но сложнее масштабировать.

Выводы и рекомендации

RBAC рекомендуется использовать в сценариях, где:

- Доступ к данным ограничивается на уровне ролей.
- Требуется простота настройки и высокая производительность.
- Организация уже использует Azure AD.

RLS рекомендуется использовать в сценариях, где:

- Требуется тонкий контроль доступа на уровне строк.

- Данные имеют высокий уровень конфиденциальности.
- Организация готова инвестировать время и ресурсы в настройку и поддержку.

Таким образом, можно сделать вывод, что выбор между использованием RBAC и RLS зависит от конкретных требований бизнеса. RBAC подходит для большинства сценариев, где требуется управление доступом на уровне ролей, а RLS — для более сложных случаев с необходимостью ограничения доступа на уровне строк. Оба механизма могут использоваться совместно для достижения максимального уровня безопасности данных в Power Apps.

Список литературы:

1. Кононов, Д. Д Обеспечение непротиворечивости расширенной ролевой модели безопасности на основе RBAC. URL: https://cyberleninka.ru/article/n/obespechenie-neprotivorechivosti-rasshirennoy-rolevoy-modeli-bezopasnosti-na-osnove-rbac/viewer (дата обращения 25.02.25)
2. Кононов, Д. Д. Параметрическое разграничение доступа в расширенной ролевой модели безопасности на основе RBAC. URL: https://cyberleninka.ru/article/n/parametricheskoe-razgranichenie-dostupa-v-rasshirennoy-rolevoy-modeli-bezopasnosti-na-osnove-rbac (дата обращения 25.02.25)
3. Вход в систему с помощью совместной работы B2B Azure. URL: https://learn.microsoft.com/ru-ru/power-apps/maker/canvas-apps/sign-in-to-power-apps#sign-in-using-azure-b2b-collaboration (дата обращения 25.02.25)
4. Аутентификация в службах Power Platform. URL: https://learn.microsoft.com/ru-ru/power-platform/admin/security/authenticate-services (дата обращения 25.02.25)
5. Подключение и аутентификация в источниках данных. URL: https://learn.microsoft.com/ru-ru/power-platform/admin/security/connect-data-sources (дата обращения 25.02.25)
6. Грачев, В.М. Механизмы защиты данных, реализованные в базе данных с универсальной моделью URL: https://cyberleninka.ru/article/n/mehanizmy-zaschity-dannyh-realizovannye-v-baze-dannyh-s-universalnoy-modelyu (дата обращения 25.02.25)
7. Philip Seamark, Row-Level Security URL: https://link.springer.com/chapter/10.1007/978-1-4842-4897-3_11 дата обращения 25.02.25)
8. Безопасность в Microsoft Power Platform. URL: https://learn.microsoft.com/ru-ru/power-platform/admin/security/overview (дата обращения 25.02.25)
9. Защита приложения и данных. URL: https://learn.microsoft.com/ru-ru/power-apps/guidance/planning/security (дата обращения 25.02.25).

References:

1. Kononov, D. D. Ensuring the consistency of an extended RBAC-based security role model. URL: https://cyberleninka.ru/article/n/obespechenie-neprotivorechivosti-rasshirennoy-rolevoy-modeli-bezopasnosti-na-osnove-rbac/viewer (accessed on 25.02.25)

2. Kononov, D. D. Parametric access control in an extended role-based security model based on RBAC. URL: https://cyberleninka.ru/article/n/parametricheskoe-razgranichenie-dostupa-v-rasshirennoy-rolevoy-modeli-bezopasnosti-na-osnove-rbac (дата обращения 25.02.25)
3. Login using Azure B2B Collaboration. URL: https://learn.microsoft.com/ru-ru/power-apps/maker/canvas-apps/sign-in-to-power-apps#sign-in-using-azure-b2b-collaboration (accessed on 25.02.25)
4. Authentication to Power Platform services. URL: https://learn.microsoft.com/ru-ru/power-platform/admin/security/authenticate-services (accessed on 25.02.25)
5. Connecting and authenticating to data sources. URL: https://learn.microsoft.com/ru-ru/power-platform/admin/security/connect-data-sources (accessed on 25.02.25)
6. Grachev, V.M. Data protection mechanisms implemented in a database with a universal model. URL: https://cyberleninka.ru/article/n/mehanizmy-zaschity-dannyh-realizovannye-v-baze-dannyh-s-universalnoy-modelyu (accessed on 25.02.25)
7. Philip Seamark, Row-Level Security URL: https://link.springer.com/chapter/10.1007/978-1-4842-4897-3_11 (accessed on 25.02.25)
8. Security in Microsoft Power Platform. URL: https://learn.microsoft.com/ru-ru/power-platform/admin/security/overview (accessed on 25.02.25)
9. Application and data protection. URL: https://learn.microsoft.com/ru-ru/power-apps/guidance/planning/security (accessed on 25.02.25)