МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ОДЕССКИЙ Национальный политехнический университет

Институт компьютерных систем

Кафедра Информационных технологий

GRID технологии

Вариант №12

Тема: «Взаимодействие между ролями в Azure.»

Выполнил:

студент группы АД-171

Надводский В.В.

Проверил:

Гришин С.И.

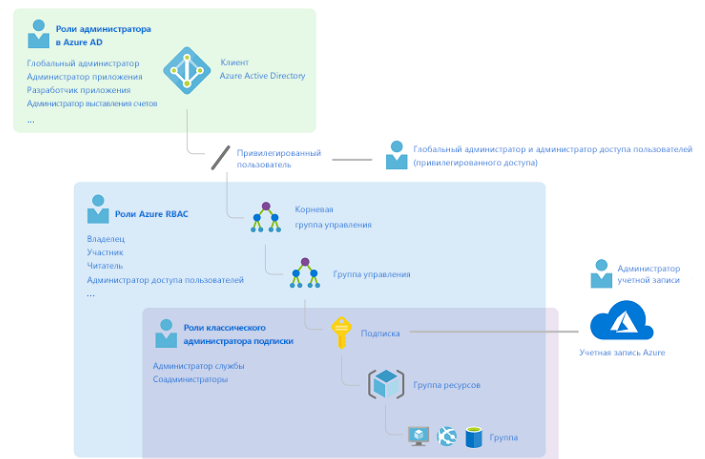
Одесса 2019

**Роли классического администратора подписки, роли RBAC Azure и роли администратора Azure AD**

Если вы еще не знакомы с Azure, понимание вопросов, связанных с ролями в Azure, может показаться вам достаточно сложным. В этой статье описываются следующие роли и приводятся рекомендации по их использованию:

* Роли классического администратора подписки
* Роли управление доступом на основе ролей в Azure (RBAC)
* Роли администратора Azure Active Directory (Azure AD)

## Взаимосвязи между ролями

Для лучшего понимания ролей в Azure требуется определенная историческая справка. В первоначальном выпуске Azure для управления доступом к ресурсам использовались всего три роли администратора: администратор учетной записи, администратор служб и соадминистратор. Впоследствии была добавлена роль управления доступом на основе ролей (RBAC) для ресурсов Azure. RBAC Azure — это новая система авторизации, которая обеспечивает более точное управление доступом к ресурсам Azure. Система RBAC включает множество встроенных ролей, которые могут назначаться в различных областях, а также позволяет создавать собственные пользовательские роли. Для управления такими ресурсами Azure AD, как пользователи, группы и домены, используется несколько ролей администратора Azure AD.

**В Azure предусмотрено три роли классического администратора** **подписки:** **администратор учетной записи, администратор службы и соадминистратор.**

Классические администраторы подписки имеют полный доступ к подписке Azure. Они могут управлять ресурсами с помощью портала Azure, интерфейсов API Azure Resource Manager и классической модели развертывания Azure. Учетной записи, используемой для регистрации в Azure, автоматически назначается роль администратора учетной записи и администратора службы. Дополнительные роли соадминистратора можно добавить уже позже.Администратор служб и соадминистратор имеют эквивалентные права доступа для пользователей, которым была назначена роль владельца (роль RBAC Azure) в области действия подписки. В следующей таблице представлены различия между этими тремя ролями классического администратора подписки.

### **Учетная запись Azure и подписки Azure**

Учетная запись Azure представляет собой отношение выставления счетов. Учетная запись Azure представляет собой удостоверение пользователя, одну или несколько подписок Azure и связанный набор ресурсов Azure. Пользователь, создавший учетную запись, является администратором учетной записи для всех создаваемых в ее рамках подписок. Этот пользователь также по умолчанию назначается администратором служб для этой подписки.

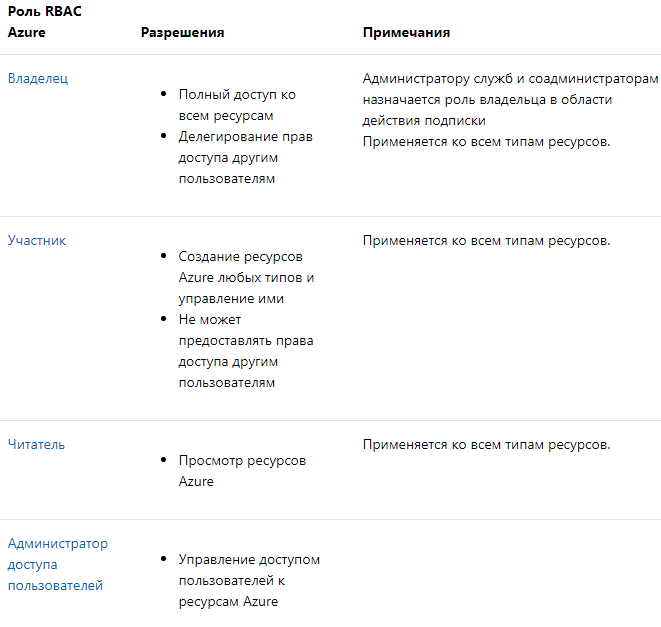
Подписки Azure служат для организованного доступа к ресурсам Azure. Они также позволяют управлять составлением отчетов об использовании ресурса, выставлением счетов за использование и их оплатой. Каждая подписка может иметь различные настройки для выставления счетов и их оплаты, поэтому у вас могут быть разные подписки и тарифные планы для разных офисов, отделов, проектов и т. д. Каждая служба привязана к подписке, идентификатор которой может требоваться для выполнения программных операций. 

Рис. 1 - Azure доступы

Остальные встроенные роли разрешают управление определенными ресурсами Azure.Например, роль [Участник виртуальных машин](https://docs.microsoft.com/ru-ru/azure/role-based-access-control/built-in-roles#virtual-machine-contributor) позволяет пользователю создавать виртуальные машины и управлять ими. Полный список встроенных ролей см. в статье [Встроенные роли для ресурсов Azure](https://docs.microsoft.com/ru-ru/azure/role-based-access-control/built-in-roles).

**Модель RBAC поддерживается только порталом Azure и API-интерфейсами Azure Resource Manager**.

 Пользователи, группы и приложения, которым назначены роли RBAC, не могут использовать [API классической модели развертывания Azure](https://docs.microsoft.com/ru-ru/azure/azure-resource-manager/resource-manager-deployment-model).

На портале Azure сведения о назначении ролей RBAC отображаются в колонке **Управление доступом (IAM)**. Эта колонка представлена в различных разделах портала, в том числе в группах управления, подписках, группах ресурсов и различных ресурсах.

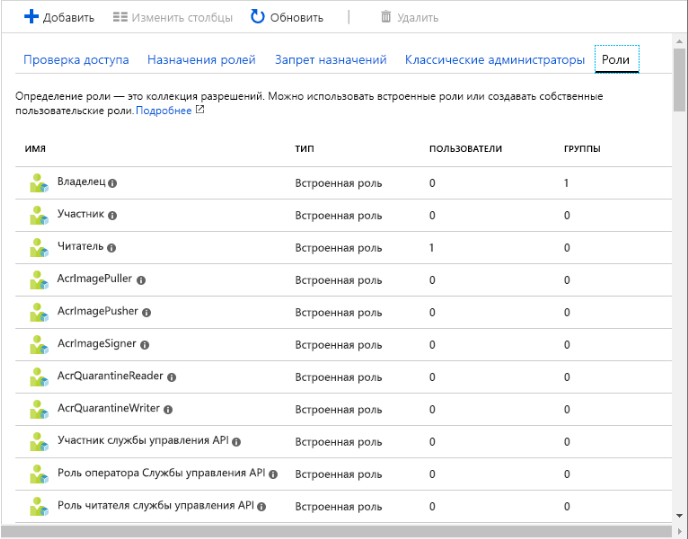
При выборе вкладки **Роли** отобразится список встроенных и пользовательских ролей.

Рис. 2 - пользовательских роли

## **Роли администратора в Azure AD**

Роли администратора Azure AD используются для управления ресурсами.

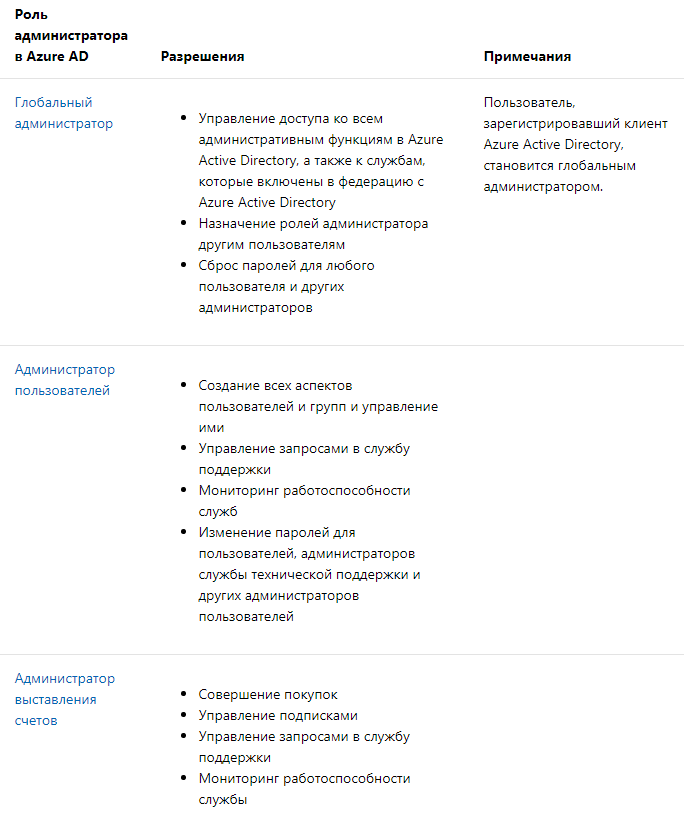
Azure AD в каталоге, то есть для создания и изменения пользователей, назначения ролей администратора другим пользователям, сброса паролей пользователей, управления лицензиями пользователей, а также для управления доменами. В следующей таблице описываются некоторые основные роли администратора Azure AD.

Рис. 3 - Список ролей администратора

Azure AD можно просмотреть в колонке **Роли и администраторы** на портале Azure. Полный список ролей администратора Azure AD см. в статье [Разрешения роли администратора в Azure Active Directory](https://docs.microsoft.com/ru-ru/azure/active-directory/users-groups-roles/directory-assign-admin-roles).

### Пересекаются ли роли RBAC Azure и роли администратора Azure AD?

## Различия между ролями RBAC Azure и ролями администратора Azure AD

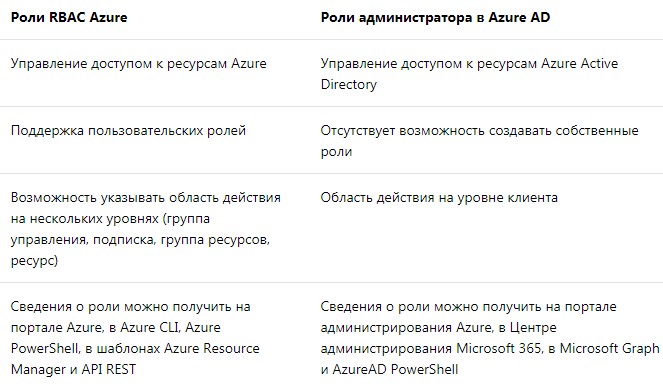
На верхнем уровне роли RBAC Azure управляют разрешениями на управление ресурсами Azure, а роли администратора Azure AD управляют разрешениями на управление ресурсами Azure Active Directory.  

Рис. 4 - Сравнение различий приводится в следующей таблице.

По умолчанию действие ролей RBAC Azure и ролей администратора Azure AD не распространяется на Azure и Azure AD. Тем не менее, если глобальный администратор повысит свой уровень доступа с помощью параметра **Глобальный администратор может управлять подписками Azure и группами управления**на портале Azure, глобальному администратору будет назначена роль [Администратор доступа пользователей](https://docs.microsoft.com/ru-ru/azure/role-based-access-control/built-in-roles#user-access-administrator) (роль RBAC) для всех подписок соответствующего клиента. Роль администратора доступа пользователей позволяет предоставлять другим пользователям доступ к ресурсам Azure. Этот параметр может использоваться для восстановления доступа к подписке. Дополнительные сведения см. в разделе [Повышение уровня доступа в качестве администратора Azure AD](https://docs.microsoft.com/ru-ru/azure/role-based-access-control/elevate-access-global-admin).

Некоторые роли администратора Azure AD, например глобальный администратор или администратор пользователей, действуют в отношении Azure AD и Microsoft Office 365.Например, если вам назначена роль глобального администратора, у вас будут права глобального администратора в отношении Azure AD и Office 365, позволяющие, например, вносить изменения в Microsoft Exchange и Microsoft SharePoint. Тем не менее по умолчанию у глобального администратора отсутствуют права доступа к ресурсам Azure.