vitextra

СТАТЬЯ БАЗЫ ЗНАНИЙ

Разрешения Microsoft Graph, необходимые для Employee Directory



2026 © Vitextra SIA. Все права защищены.

Отказ от ответственности

Для целей настоящего Заявления об отказе от ответственности:

- **Компания** (именуемая в данном Отказе от ответственности "Компания", "Мы", "Нас" или "Наш") относится к Vitextra SIA, LV-1009 Riga, Matise iela 61 - 25.
- **Документ** ссылается на статью Базы знаний.
- **Вы** означает физическое лицо, получающее доступ к Документу, или компанию, или другое юридическое лицо, от имени которого такое физическое лицо получает доступ к Документу или использует его, в зависимости от обстоятельств.
- **Веб-сайт** относится к Vitextra, доступному с https://vitextra.com

Отказ от ответственности

Информация, содержащаяся в Документе, предназначена только для общих информационных целей.

Компания не несет ответственности за ошибки или упущения в содержании Документа.

Ни в коем случае Компания не несет ответственности за какие-либо особые, прямые, косвенные, логически вытекающие или случайные убытки или любой ущерб вообще, будь то в результате действия договора, халатности или других правонарушений, возникающих в результате или в связи с использованием содержания Документа. Компания оставляет за собой право вносить дополнения, удаления или модификации в содержание Документа в любое время без предварительного уведомления.

Отказ от ответственности за ошибки и упущения

Информация, представленная в Документе, предназначена только для общего руководства по вопросам, представляющим интерес. Таким образом, ошибки могут возникать, даже если Компания принимает все меры предосторожности для обеспечения актуальности и точности содержания Документа. Кроме того, учитывая меняющийся характер законов, правил и подзаконных актов, могут возникнуть задержки, упущения или неточности в информации, содержащейся в Документе.

Компания не несет ответственности за какие-либо ошибки или упущения, а также за результаты, полученные в результате использования этой информации.

Отказ от добросовестного использования

Компания может использовать защищенные авторским правом материалы, которые владелец авторских прав явно не разрешил. Компания делает такие материалы доступными для критики, комментариев, новостных репортажей, преподавания, стипендий или исследований.

Компания считает, что это представляет собой "добросовестное использование" любого такого защищенного авторским правом материала, как это предусмотрено в разделе 107 закона США об авторском праве.

Если Вы хотите использовать защищенные авторским правом материалы из Документа в своих собственных целях, выходящих за рамки добросовестного использования, Вы должны получить разрешение от владельца авторских прав.

Отказ от ответственности "Используйте на Свой Страх и Риск"

Вся информация в Документе предоставляется "как есть", без каких-либо гарантий полноты, точности, своевременности или результатов, полученных в результате использования этой информации, и без каких-либо гарантий, явных или подразумеваемых, включая, но не ограничиваясь гарантиями производительности, товарной пригодности и пригодности для конкретного цель.

Компания не несет ответственности перед Вами или кем-либо еще за любое принятое решение или действие, основанное на информации, предоставленной Сервисом, или за любые косвенные, особые или аналогичные убытки, даже если она предупреждена о возможности таких убытков.

Свяжитесь с Нами

Если у вас есть какие-либо вопросы по поводу этого заявления об отказе от ответственности, Вы можете связаться с нами по электронной почте: support@vitextra.com .

Оглавление

Введение 4

Разрешения 4

Делегированные, а не разрешения приложения 6

Источник «Профили пользователей» и поиск SharePoint 6

Что видят пользователи, если разрешения нет 7

Утверждение разрешений 10

Проверка состояния разрешений 10

Заметки для проверки безопасности 11

Термины 12

Введение

Решение Vitextra Employee Directory не ведёт собственную базу данных сотрудников. Люди, атрибуты профилей, фотографии, руководители, присутствие в Teams и сведения о занятости считываются из **Microsoft 365** во время работы через **Microsoft Graph** API. Для этого пакет решения запрашивает пять разрешений Microsoft Graph, которые администратор клиента утверждает один раз.

В этой статье перечислены эти разрешения, объяснено, для чего используется каждое из них и какой веб-части оно нужно, точно описано, что видят пользователи, если разрешение не утверждено, и показано, как утвердить разрешения и проверить их состояние. Статья предназначена для администраторов **SharePoint** и Microsoft 365, а также для специалистов по безопасности, которые оценивают продукт перед развёртыванием.

Разрешения

Пакет **Vitextra Employee Directory** содержит три веб-части - **Employee Directory**, **Employee Directory (Entra ID)** и **New Employees** - и запрашивает для них один общий набор разрешений. Все пять - **делегированные разрешения** Microsoft Graph:

Разрешение	Для чего используется	Где нужно	Если не утверждено
`Directory.Read.All`	Чтение участников ролей каталога Microsoft Entra для условия **Роли пользователей** в редакторе фильтров. Вместе с `User.Read.All` оно также позволяет читать учётные записи пользователей	Employee Directory (Entra ID), New Employees - только если в фильтре есть условие **Роли пользователей**	Если настроен фильтр по ролям, Employee Directory (Entra ID) показывает предупреждение и не может достоверно проверить членство в ролях; New Employees показывает ошибку.
`User.Read.All`	Чтение и поиск учётных записей пользователей и атрибутов их	Все три веб-части; в веб-части **Employee Directory** с источником	**Список** людей не загружается, и отображается ошибка (см. **ниже**)

Разрешение	Для чего используется	Где нужно	Если не утверждено
	профилей, руководителя и прямых подчинённых человека, команды текущего пользователя, а также фотографий сотрудников	**Профили пользователей** - фотографии, панель сведений и быстрые фильтры	
`Presence.Read.All`	Индикатор присутствия **Microsoft Teams** на карточках, столбец **Состояние** и сообщение **Нет на месте** в панели сведений	Все три веб-части	Люди отображаются без присутствия; в столбце **Состояние** указано **Не в сети**
`Calendars.Read`	Расписание занятости человека и текущего пользователя на сегодня вместе с часовым поясом и рабочими часами человека	Employee Directory, Employee Directory (Entra ID) - панель сведений	Раздел **Местное время**, **Рабочие часы** и **Доступность** не отображается
`People.Read`	Список людей, с которыми текущий пользователь работает чаще всего	Employee Directory, Employee Directory (Entra ID) - быстрый фильтр **Люди, с которыми я работаю**	Вкладка **Люди, с которыми я работаю** не отображается

Примечание

Разрешения `Directory.Read.All` и `User.Read.All` пересекаются: для чтения учётных записей пользователей Microsoft Graph принимает любое из них. Поэтому ошибка, описанная в строке `User.Read.All`, возникает, когда не утверждено ни одно из них, - это обычное состояние сразу после развёртывания, пока все пять запросов ещё ожидают утверждения. Утвердите оба разрешения, как того требует пакет.

Employee Directory использует эти разрешения только для **чтения** данных каталога, профилей и почтовых ящиков в **Microsoft Entra ID** и Microsoft 365. Решение не изменяет эти данные и не запрашивает разрешений со словом *Write* в названии. Сохранение настроек веб-части на странице SharePoint не связано с этими разрешениями Microsoft Graph.

Делегированные, а не разрешения приложения

Все пять разрешений - **делегированные**: каждый вызов Microsoft Graph выполняется из браузера вошедшего пользователя с маркером, выданным этому пользователю. У веб-частей нет разрешений приложения (app-only), нет служебной учётной записи и нет собственного серверного компонента, который читал бы ваш каталог.

Microsoft Graph учитывает выданные делегированные разрешения вместе с правами текущего пользователя. Поэтому состав каталога может отличаться от людей, видимых в Outlook или Teams: это не копия их адресных книг.

Примечание

Разрешения предоставляются не самому пакету Employee Directory. SharePoint предоставляет их одному приложению Microsoft Entra ID, которое используется для всех решений SPFx в клиенте, - *Web Client Extensibility* (ранее: *SharePoint Online Client Extensibility Web Application Principal*). Если разрешение уже утверждено для другого решения, например для Vitextra Organizational Chart, используется то же самое предоставление, и запрос больше не появляется как ожидающий. То же утверждение действует и тогда, когда веб-части работают в Microsoft Teams.

Источник «Профили пользователей» и поиск SharePoint

Веб-часть **Employee Directory** может получать людей из двух источников, которые выбираются в её параметрах:

- **Entra ID (Azure AD)** - список, поиск и разбиение на страницы работают через Microsoft Graph и зависят от перечисленных выше разрешений.
- **Профили пользователей** - список, поиск, уточнения и сортировка берутся из **поиска SharePoint** (результаты по людям службы поиска SharePoint), а не из Microsoft Graph. Они работают с собственными правами пользователя на поиск SharePoint с обычным отсечением по правам доступа и не требуют ни одного разрешения Microsoft Graph. Раздел **Последние документы** в панели сведений также использует поиск SharePoint.

Даже с источником **Профили пользователей** некоторые части веб-части по-прежнему обращаются к Microsoft Graph: фотографии, присутствие и сообщение **Нет на месте**, разделы **Руководитель** и **Прямые подчинённые** и раздел **Местное время**, **Рабочие часы** и **Доступность** в панели сведений, а также быстрые фильтры **Моя команда** и **Люди, с которыми я работаю**. Они зависят от тех же разрешений, что и в режиме **Entra ID (Azure AD)**.

Веб-части **Employee Directory (Entra ID)** и **New Employees** всегда используют Microsoft Graph.

Подсказка

О различиях между двумя веб-частями каталога и их источниками см. статью KB10310. Employee Directory или Employee Directory (Entra ID): какую веб-часть выбрать.

Что видят пользователи, если разрешения нет

Веб-части устроены так, что отсутствие необязательного разрешения отключает только зависящую от него функцию. Точное поведение в текущей версии:

Веб-часть / режим	Отсутствующее разрешение	Что видят пользователи
Employee Directory (Entra ID)	`User.Read.All` (и `Directory.Read.All`)	При первоначальной загрузке, если ранее загруженного непустого списка нет: Вместо списка - значок ошибки с текстом ошибки, который

Веб-часть / режим	Отсутствующее разрешение	Что видят пользователи
		вернул Microsoft Graph; если текста нет - сообщение *К сожалению, произошла непредвиденная ошибка. Обновите страницу и повторите попытку.*
Employee Directory, источник **Entra ID (Azure AD)**	`User.Read.All` (и `Directory.Read.All`)	Та же ошибка вместо результатов поиска
Employee Directory, источник **Профили пользователей**	`User.Read.All` (и `Directory.Read.All`)	Список, поиск и уточнения продолжают работать. В панели сведений не отображаются разделы **Руководитель** и **Прямые подчинённые**, а фотографии берутся из SharePoint, а не из Microsoft Graph
New Employees	`User.Read.All` (и `Directory.Read.All`)	Значок ошибки с сообщением *К сожалению, произошла непредвиденная ошибка. Обновите страницу и повторите попытку.*, за которым следует текст ошибки, возвращённый Microsoft Graph
Employee Directory (Entra ID), New Employees	`Directory.Read.All`	Если настроен фильтр по ролям, Employee Directory (Entra ID) показывает предупреждение и не может достоверно проверить членство в

Веб-часть / режим	Отсутствующее разрешение	Что видят пользователи
		ролях; New Employees показывает ошибку.
Все веб-части	`Presence.Read.All`	На карточках нет индикатора присутствия, в столбце **Состояние** у всех указано **Не в сети**, а в панели сведений нет сообщения **Нет на месте**
Employee Directory, Employee Directory (Entra ID)	`Calendars.Read`	Раздел **Местное время**, **Рабочие часы** и **Доступность** в панели сведений не отображается. Ошибка не отображается
Employee Directory, Employee Directory (Entra ID)	`People.Read`	Вкладка **Люди, с которыми я работаю** скрыта на панели быстрых фильтров. Остальные вкладки продолжают работать

Предупреждение

Веб-часть **Employee Directory (Entra ID)** хранит копию загруженного списка в браузере и показывает её при следующем посещении. Когда копия становится старше 24 часов, запускается фоновое обновление; кнопка **Обновить** также запускает новый запрос. Если после отзыва разрешения запрос завершается ошибкой, а ранее загруженный непустой список уже отображается, веб-часть сохраняет список и исходную дату его обновления. Появляется предупреждение: *Не удалось обновить список. Показана сохранённая копия.*, за которым следует текст ошибки, если он доступен. Экран ошибки не заменяет список. Он появляется, если загрузка завершается ошибкой и ранее загруженного непустого списка нет. Проверяя изменение разрешений, очистите данные сайта в браузере или используйте приватное окно.

Примечание

Для присутствия и сведений о занятости одного разрешения недостаточно: чтобы у человека было состояние присутствия, он должен пользоваться Microsoft Teams, а чтобы было расписание занятости - иметь почтовый ящик Exchange Online. Подробнее о разделе доступности см. статью KB10317. Employee Directory: местное время, рабочие часы и доступность, о быстрых фильтрах - статью KB10214. Быстрые фильтры Employee Directory: мой отдел, моя команда, люди, с которыми я работаю, избранное.

Утверждение разрешений

Запросы разрешений создаются автоматически, когда пакет Employee Directory развёртывается в каталоге приложений клиента. Их утверждает **Глобальный администратор**:

1 Откройте **Центр администрирования SharePoint**.
2 В области навигации слева разверните раздел **Дополнительно** и выберите **Доступ к API**.
3 На вкладке **Ожидающие запросы** найдите запросы пакета **Vitextra Employee Directory** к **Microsoft Graph** - `Directory.Read.All`, `User.Read.All`, `Presence.Read.All`, `Calendars.Read` и `People.Read`.
4 Выберите каждый запрос, нажмите **Утвердить** и подтвердите.

Пользователи не видят запроса на согласие: после утверждения веб-части работают у всех в клиенте. Если через несколько минут после утверждения веб-часть всё ещё показывает ошибку, обновите страницу.

Подсказка

Полная процедура, включая утверждение с помощью PowerShell, частичное утверждение и отзыв разрешений, описана в статье KB10360. Как одобрить разрешения Microsoft Graph API для решений Vitextra в Центре администрирования SharePoint.

Проверка состояния разрешений

Чтобы проверить, какие разрешения действуют, откройте **Дополнительно** › **Доступ к API** в Центре администрирования SharePoint:

- На вкладке **Утвержденные запросы** должны быть перечислены все пять

разрешений Microsoft Graph. Поскольку предоставления действуют на весь клиент, разрешение может быть указано там под другим пакетом, который запросил его первым, - этого достаточно.
- Любое разрешение, которое всё ещё указано на вкладке **Ожидающие запросы**, пока не действует; функции, которые от него зависят, ведут себя так, как описано в разделе **Что видят пользователи, если разрешения нет**.

При обновлении Employee Directory ранее утверждённые разрешения остаются утверждёнными. Если новая версия запрашивает дополнительное разрешение, оно появляется на вкладке **Ожидающие запросы**, и его нужно утвердить тем же способом.

Заметки для проверки безопасности

Для проверки безопасности обычно важны следующие моменты:

- Все пять разрешений Microsoft Graph делегированные и предназначены только для чтения; они не позволяют Employee Directory изменять данные каталога, профилей или почтовых ящиков.
- Данные каталога, фотографии, присутствие и сведения календаря запрашиваются браузером пользователя напрямую из Microsoft Graph и SharePoint и не передаются ни Vitextra, ни третьим лицам.
- Источник **Профили пользователей** читает людей через поиск SharePoint с правами самого пользователя, и для самого списка ему не нужно ни одного разрешения Microsoft Graph.
- Избранное, кэшированный список сотрудников и конфигурация по умолчанию для личного приложения Teams хранятся вне Microsoft Graph; где именно и какие данные читают веб-части, описано в статье KB10469. Employee Directory: какие данные читает веб-часть и где хранятся избранное и параметры.
- Запросы к службам Vitextra включают проверку лицензии, телеметрию использования с техническими идентификаторами и, при использовании этой функции, хранение конфигурации по умолчанию личного приложения Teams; см. KB10363. Где продукты Vitextra хранят ваши данные: конфиденциальность, расположение данных и GDPR.

Подсказка

Об установке решения см. статью KB10035. Как установить продукт Vitextra в SharePoint Online. О добавлении веб-части на страницу см. статью KB10309. Как добавить и настроить веб-часть Employee Directory.

Подробнее о продукте: *https://vitextra.com/ru/products/employee-directory*

Термины

Делегированные разрешения
Делегированные разрешения позволяют приложению действовать от имени вошедшего в систему пользователя. Фактический доступ приложения определяется пересечением разрешений, предоставленных приложению, и разрешений пользователя.

Список
Список — это единица хранения данных в SharePoint. Список может содержать столбцы разных типов, типы контента и представления. Библиотека документов — это особый тип списка, поэтому она наследует его функциональность.

Microsoft 365
Microsoft 365 — это облачная служба по подписке, объединяющая приложения для повышения производительности, такие как Word, Excel, PowerPoint и Outlook, с облачными службами, такими как SharePoint, OneDrive, Teams и Exchange Online, а также расширенные средства обеспечения безопасности и управления устройствами.

Microsoft Entra ID
Microsoft Entra ID (ранее Azure Active Directory) — это облачная служба управления удостоверениями и доступом от корпорации Майкрософт. Она позволяет организациям эффективно управлять удостоверениями пользователей и доступом к различным внутренним и внешним ресурсам, а также защищать их. К этим ресурсам относятся Microsoft 365, платформа Azure и тысячи других приложений SaaS (программное обеспечение как услуга).

Microsoft Graph
Microsoft Graph — это REST API, защищенный с помощью Microsoft Entra ID (ранее Azure Active Directory) и OAuth 2.0. Он предоставляет единую конечную точку для доступа к данным и службам Microsoft 365, таким как SharePoint, Outlook, OneDrive, Teams и другим.

Microsoft Teams
Microsoft Teams — это платформа для совместной работы на основе чата, предназначенная для деловых коммуникаций. Она включает возможности для проведения онлайн-собраний и прямых трансляций, а также для обмена

документами.

SharePoint
SharePoint — это веб-платформа для совместной работы, которая предоставляет средства управления содержимым и документами, приложения рабочих процессов, поиск и другие инструменты, помогающие сотрудникам и командам работать вместе. SharePoint также является безопасным местом для хранения общей информации, ее организации и доступа к ней.