SalesPlatform vtiger crm 620 Основы ролевой модели безопасности

Главная страница руководства

 Внимание: данная страница находится в разработке, информация может соответствовать более ранней версии системы.

Содержание

Краткий обзор

В текущей версии системы vtiger CRM внедрена *ролевая модель системы безопасности*, для определения, кто имеет право просматривать, редактировать и удалять какую информацию, хранящуюся в системе vtiger CRM. Это существенное улучшение, делающее систему vtiger CRM более масштабируемой, гибкой и легкой для внедрения в больших компаниях.

Настоящий раздел объясняет, как *начать работу с настройками безопасности vtiger CRM и как пользоваться ролевой моделью безопасности системы*. Дается обзор всех соображений, которые администратор должен обдумать до начала установки системы vtiger CRM.

Введение в ролевую модель безопасности

Работа системы vtiger CRM базируется на современном управлении безопасностью, которая использует концепцию ролей, подобную реализации систем безопасности во многих современных прикладных системах. Ролевая модель безопасности (также называемая ролевым контролем доступа) построена на условии аутентификации пользователей, то есть на процессе идентификации пользователей. Когда пользователь идентифицирован, ему назначаются роли и разрешения.

 Примечание

Ролевая модель безопасности определяет и принуждает использовать специфические политики безопасности предприятия таким путем, который естественно согласуется с организационной структурой предприятия.

Ролевая модель безопасности стала доминирующей моделью контроля доступа, так как она уменьшает сложность и стоимость администрирования безопасности.

Хотя ролевая модель безопасности может быть чересчур утяжеленной для примитивных настроек (например, в случае маленьких предприятий с нескольким пользователями, причем всем разрешено просматривать, удалять, или изменять все данные), она является чрезвычайно мощным инструментом для контроля сложных сред. Это включает типовые настройки компаний, когда различным командам отдела продаж или сотрудникам технической поддержки необходимо просматривать, удалять, или редактировать данные, относящиеся к клиентам, и в то же самое время права доступа к таким данным сильно зависят от должности или задачи сотрудника в компании. Эта концепция особенно удобна для компаний:

- которым необходимо дать *возможность большому количеству людей* работать с системой vtiger CRM одновременно,
- которым необходимо у*становить ограничения* на просмотр, удаление, или удаления для индивидуальных пользователей, и
- которым требуется *установить иерархический порядок* предоставления прав.

Хотя ролевая модель безопасности не декларирует никакой политики защиты данных, было доказано, что такая модель позволяет поддерживать некоторые хорошо известные принципы и политики, важные для коммерческих и правительственных организаций, которые обрабатывают не классифицированную, но конфиденциальную информацию. Эти политики могут быть установлены в момент, когда профили авторизованы на роль, в момента, когда роль назначена пользователю (например, когда роль установлена как часть активной сессии пользователя), или когда пользователь пытается совершить действие над данными.

Определение терминов

Определение пользователей

В системе vtiger CRM существует два типа пользователей:

- *Стандартный* пользователь
- Пользователь-*администратор*

Стандартному пользователю предоставлены ограниченные права доступа в систему vtiger CRM для выполнения *CRUD (Create (создавать), Retrieve (просматривать), Update (изменять), и Delete (удалять))*, и ограниченные, специфические только для пользователя операции настроек.

Пользователи-*администраторы* обладают возможностями *полного контроля* и управления программным обеспечением, которые включают:

- *управление* пользователями и группами и их правами доступа,
- *настройку* пользовательского интерфейса системы vtiger CRM,
- *создание* шаблонов сообщений,
- *настройку* параметров уровня организации,
- *изменение* пользовательских паролей, деактивацию (отключение от системы) пользователей, просмотр журнала регистрации пользователей в системе, и
- *выполнение* операций CRUD для любых данных.

На рис. 14.1 показан экран детального вида информации пользователя, выведенный функцией

управления пользователями системы vtiger CRM.

Рис. 14.1: Специальная функция администратора в меню Users

При установке отметки в поле *[Администратор]* пользователь получает права администратора.

Исходя из общих соображений, рекомендуется давать права Администратора одному или небольшому количеству пользователей системы.

Определение ролей

Основой ролевой модели безопасности является концепция сбора прав в *ролях*, которые потом могут быть назначены стандартным пользователям. Каждая роль базируется на одном или более профилях. Принадлежность пользователя к той или иной роли определяет разрешенные пользователю права. Администрирование безопасности в ролевой модели сводится к определению операций, выполняемых пользователями во время типовых действий, и назначению сотрудникам правильных ролей. Ролевая структура модели безопасности предоставляет как исключительные, так и перекрывающиеся права и обязанности. Например, некоторые общепринятые операции могут быть разрешены всем сотрудникам, а какие-то операции могут быть специфичными для роли. Ролевые иерархии естественно соответствуют ролевой организации внутри компании и определяют отношения и атрибуты ролей. Сложности, вызванные взаимно-исключительными ролями либо иерархиями ролей, так же как и определение, кто какие действия может совершать, регулируются ролевой моделью установок безопасности.

Одним из крупнейших преимуществ ролевой модели безопасности являются поддерживаемые ей возможности администрирования. Принадлежность пользователя к роли может быть легко назначена и отозвана, и новое назначение устанавливается в соответствии с назначенной работой. При ролевой модели безопасности пользователям не даются на индивидуальном уровне права выполнения операций, а наоборот, операции ассоциированы с ролями. Ассоциация ролей с новыми операциями либо удаление старых операция из ролевых прав может производиться по мере изменения и эволюционирования должностных обязанностей. Эта главная концепция обладает преимуществом простоты понимания и управления правами. Изменение ролей не вызывает необходимости изменения прав пользователей на индивидуальной основе.

Важно
Каждый созданный в системе vtiger CRM пользователь должен быть связан с *ролью*. Роль должна быть связана как минимум с одним *профилем*.

Более того, индивидуальные пользователи (например, John, Mary) могут быть назначены на одну или более ролей, которые базируются на обязанностях и выполняемой пользователями работы в компании. Пользователям может быть назначено несколько ролей для отражения того факта, что некоторые пользователи входят в систему для выполнения различных функций в зависимости от текущих задач. Например, пользователю

"http://wiki.salesplatform.ruJohn"http://wiki.salesplatform.ru может быть назначена роль "http://wiki.salesplatform.ruHead-Sales"http://wiki.salesplatform.ru, так как John является начальником отдела продаж в вашей компании, и роль "http://wiki.salesplatform.ruadmin"http://wiki.salesplatform.ru, так как John также является администратором системы vtiger CRM. Если John хочет работать как администратор, он заходит в систему как "http://wiki.salesplatform.ruadmin"http://wiki.salesplatform.ru, а если John хочет работать как начальник отдела продаж, он заходит в систему как "http://wiki.salesplatform.ruHead-Sales"http://wiki.salesplatform.ru. Возможно разрешить ему заходить в систему с тем же самым паролем, вне зависимости от того, действует ли он как администратор или начальник отдела продаж.

 Примечание

Пользователи с любой назначенной ролью всегда могут просматривать, изменять и удалять любые данные, принадлежащие пользователям, расположенным ниже по иерархии.

Для того, чтобы система vtiger CRM реализовала все свои возможности, как система уровня предприятия, необходимым является наличие контрольного механизма, регулирующего пользовательский доступ к информации соответственно сегодняшним требованиям вашего бизнеса. Ролевая модель безопасности допускает разработку и установление разнообразных регламентов защиты, которая может быть приспособлена для различных предприятий. Целью ролевой модели безопасности является предоставление услуги контроля доступа. Когда базовая модель ролевой безопасности для предприятия определена, дальнейшие действия по администрированию сводятся к назначению и отзыву ролей для пользователей в соответствии с должностными обязанностями пользователей. Такое обслуживание легко производится при помощи средств управления пользователями системы vtiger CRM.

Определение профилей

Профили используются в задании прав для выполнения операций системы vtiger CRM. С функциональной точки зрения, центральная идея ролевой модели безопасности заключается в том, что профили представляют собой действия, связанные с ролями, и пользователями, являющимся членами этих ролей.

Отношение между пользователями, ролями и профилями изображено на рис.15.2 как отношение многие-ко-многим.

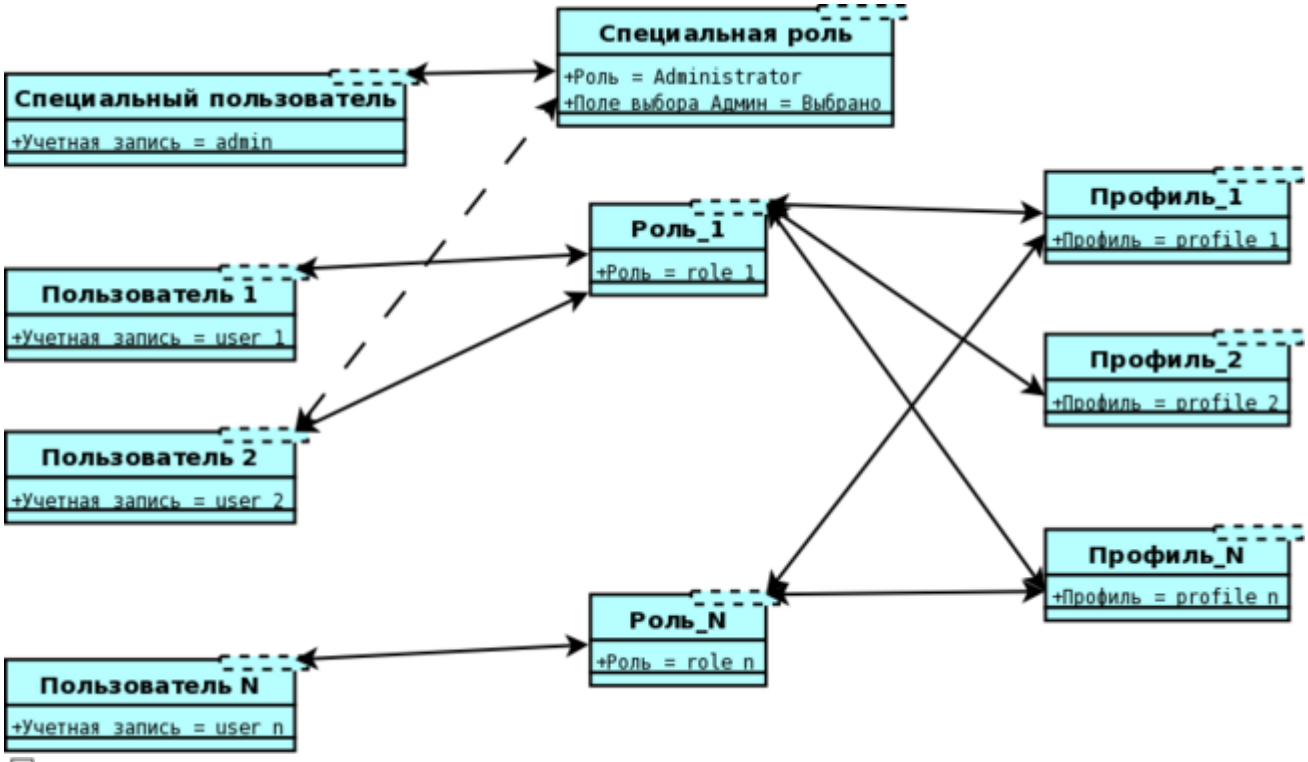


Рис. 15.2: Отношения пользователей, ролей, и профилей

Например, стандартный пользователь может быть связан с одной или более ролями посредством различных пользовательских имен, а роль может быть назначена одному или более пользователям. Роли могут создаваться для различных должностей в организации. Например, может быть создана роль для представителя отдела продаж, для ассистента, и т.п. Профили, ассоциированные с ролями, разрешают пользователям, которым назначены роли, указанный набор действий. Например, внутри отдела продаж роль представителя отдела продаж может включать операции создания, редактирования и удаления собственного контрагента, роль ассистента может быть ограничена просмотром существующей информации определенного представителя, а роль начальника отдела может предоставлять право просмотра и редактирования любых данных отдела.

Связывание профилей с ролями внутри предприятия может обеспечить самодостаточность ролей. Профили могут быть заданы способом, который используется для демонстрации и обеспечения выполнения требований инструкций. Например, обязанности ассистента могут быть ограничены добавлением новых записей в журнал активности по клиентам, а не редактированием записей продаж.

Базирующиеся на профилях права доступа устанавливает организатор системы vtiger CRM, когда настраивает систему. Доступны следующие типы прав доступа:

- Право использования определенных модулей системы vtiger CRM.
- Право просмотра данных в определенных модулях системы vtiger CRM.
- Право редактирования или изменения данных в определенных модулях системы vtiger CRM.
- Право удаления данных в определенных модулях системы vtiger CRM.
- Право экспорта данных из определенных модулей системы vtiger CRM.
- Право импорта данных в в определенные модули системы vtiger CRM.

Система vtiger CRM дает пользователю возможность совершения только тех операций, на которые пользователю даны права.

Важно

Учитывайте следующие общие правила:

- Специальные права всегда преобладают над общими правами
- Аннулированные права всегда накладываются на данные права
- В системе vtiger CRM существуют специальные правила. См. примечания, отмеченные словом **Важно**

Система vtiger CRM различает следующие типы прав:

Таблица 15.1: Типы прав в профиле

Тип прав	Описание
Глобальные права	Когда вы создаете профиль, глобальные права позволяют вам установить, даются ли общие права на просмотр и редактирование всей информации / всех модулей системы vtiger CRM: • *View all (видеть все):* Пользователь, роль которого базируется на данном профиле, позволяющем видеть все данные, сможет просматривать все данные всей организации. Вам не следует давать такое право, если вы планируете внедрить разграничение прав доступа. • *Edit all (редактировать все):* Пользователь, роль которого базируется на данном профиле, позволяющем видеть все данные, сможет создавать / просматривать все данные всей организации. Вам не следует давать такое право, если вы планируете внедрить разграничение прав доступа. Важно Глобальные права в профилях главнее разрешений, установленных в описанных ниже правах на Закладки, Стандартные права, Правах на Поля и Правах на Утилиты. Предположим, например, что доступ к закладке Сделки запрещен через права Права на закладки. Даже в этом случае пользователь может просматривать данные модуля Сделки, если ему установлено разрешение *Видеть все* в разделе *Глобальные права* в его профиле.
Права на закладки	Опция определения прав на закладки интерфейса позволяет задавать, какие закладки или модули будут доступны пользователю. Система vtiger CRM предлагает выбор из списка всех имеющихся модулей.
Права на поля	Эта опция служит для установки стандартных привилегий и позволяет вам давать права *Создавать*, *Редактировать*, *Удалять*, и *Просматривать* на уровне полей системы vtiger CRM. Система vtiger CRM предлагает выбор из списка всех имеющихся полей. Важно Пользовательские поля также включены в список. Соответственно, рекомендуется создать все необходимые пользовательские поля до начала установки прав доступа к полям.
Утилиты	Многочисленные модули системы vtiger CRM поставляются с функциями утилит, такими, как *Импорт*, *Экспорт*, *Объединение – для групповых писем*, и *Преобразование обращений*. Опция установки прав на утилиты позволяет вам определять, какие функции утилит доступны базирующейся на соответствующем профиле роли.

Важно

Права, определенные в профилях, преобладают над правами, установленными в *Default*

Organization Sharing Rules (права доступа организации по умолчанию) и *User defined Sharing Rules (права пользователя)*.

Предположим, например, что права доступа организации позволяют пользователю видеть *Сделки* иных пользователей. Однако, если профиль не позволяет получать доступ к модулю *Сделки*, эти права доступа аннулируются.

Определение групп

Для лучшей управляемости система vtiger CRM позволяет объединять пользователей, роли, роли с субординацией, и группы пользователей в группы. Важно понимать, что группы не являются средством создания настроек безопасности. Группы скорее используются для управления доступом к данным.


Важно

Учтите, что установки для группы преобладают над установками для профилей. Права группы могут быть ограничены правами доступа на уровне организации.

Группа пользователей

Система vtiger CRM предоставляет функции для создания групп пользователей, иногда также называемых командами. Пример группы, названный *Команда А*, показан на рис. 15.3.

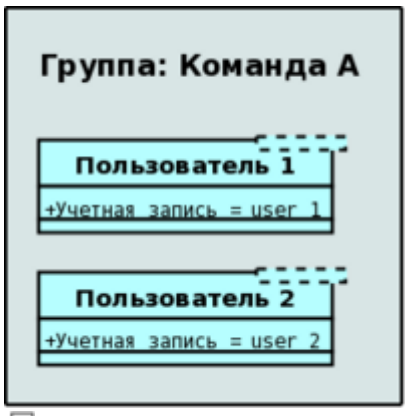


Рис. 15.3: Пример группы пользователей

Вы можете давать этим группам любые названия и включать в группу неограниченное количество пользователей.

Группа ролей

Вы также можете построить *группы*, основанные на *ролях*. Пример показан на рис. 15.4.

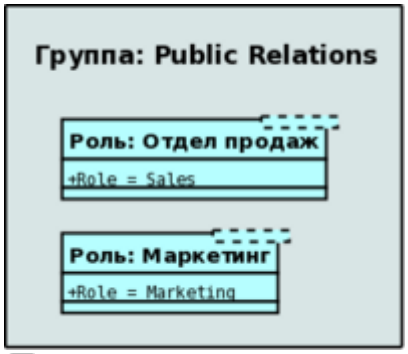


Рис. 15.4: Пример группы ролей

Это может быть полезно , если вы не знаете отдельных пользователей и их должностных обязанностей в компании.

В показанной группе все пользователи, являющиеся членами ролей *Sales (Отдел продаж)* или *Marketing (маркетинг)*, включены в показанную группу *Public Relations*. Если вы назначите эту группу ответственной за какую-либо запись в системе vtiger CRM, все члены группы станут ответственными за запись.

Группа ролей с субординацией

Кроме групп, базирующихся на простых ролях, вы также можете построить группы, которые включают субординацию. Это означает, что пользователи, которым назначены роли, подчиняющиеся включенной в группу роли, также будут включены в группу. Это проиллюстрировано ниже. Предположим, иерархический порядок в вашей компании установлен, как показано на рис. 15.5.

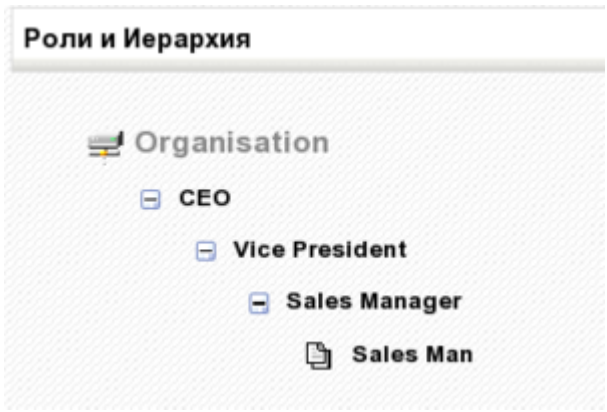


Рис. 15.5: Пример иерархии

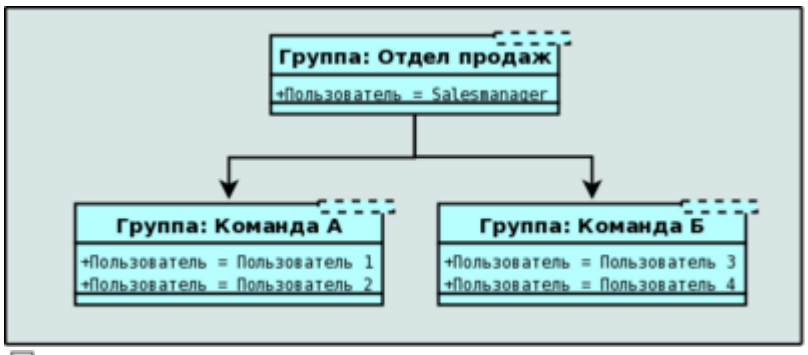
На приведенном рисунке у роли *Sales Manager (Руководитель отдела Продаж)* в подчинении роль *Sales Man (Продавец)*, а роль *Sales Manager (Руководитель отдела Продаж)* подчиняется роли *Vice President (Вице-президент)*.

Если создать пользовательскую группу, как показано на рис. 15.6, все пользователи с ролями, относящимися к *sales (продажи)* и *marketing (маркетинг)*, включая ассистентов, станут членами этой новой группы.

Рис. 15.6: Группа ролей с субординацией - пример

Группы групп

Вы можете строить группы, членами которых также являются группы. Это означает, что все пользователи, являющиеся членами выбранной группы, станут также членами новой группы. Предположим, вы хотите построить иерархическую структуру, показанную на рис. 15.7. Базируясь на данной структуре, вы можете построить пользовательскую группу *Sales (продажи)*, членами которой являются группы *Команда А* и *Команда Б*. В данном примере членами групп *Команда А* и *Команда Б* являются отдельные пользователи.



Рисю 15.7: Пример иерархии для групп

Если вы назначили ответственным за некоторую запись в системе vtiger CRM группу *Sales (Продажи)*, то *Пользователи 1* до *4* все будут являться ответственными за эту запись с соответствующими правами.

Главная страница руководства