Глава 11

Контроль доступа, лицензирование и конфигурирование

В этой главе

- Введение
- Обзор подсистемы контроля доступа
- Разработка артефактов контроля доступа
- Проверка артефактов контроля доступа
- Создание политик Extensible Data Security
- Написание защищенного кода
- Лицензирование и конфигурирование

Введение

В Microsoft Dynamics AX 2012 появилась новая подсистема контроля доступа, основанная на модели роле-ориентированного контроля доступа. Эта подсистема разработана таким образом, чтобы облегчить поддержку настроек контроля доступа по мере того, как потребности организации в его обеспечении эволюционируют. Она также облегчает процесс реализации минимально допустимого уровня контроля доступа.

Системные администраторы и разработчики управляют своими элементами новой системы контроля доступа. Разработчики создают и определяют артефакты контроля доступа, предоставляющие доступ к защищаемым объектам, а системные администраторы управляют правами доступа пользователей на непрерывной основе.

В этой главе описывается, как среда времени выполнения Microsoft Dynamics AX реализует функции контроля доступа, лицензирования и конфигурирования, и объясняется, как они определяют те области интерфейса, которые пользователь видит, и те данные, к которым он может получить доступ. Вы можете использовать подсистему контроля доступа для

создания соответствующих артефактов, контролирующих доступ к формам, отчетам, меню и отдельным пунктам меню. Также в Microsoft Dynamics AX 2012 появилась новая расширяемая подсистема контроля доступа к данным (extensible data security framework), позволяющая вам на детальном уровне ограничить доступ к важным данным, чтобы пользователи видели лишь данные, с которыми им непосредственно нужно работать.

Подсистемы лицензирования и конфигурирования дают возможность лицензировать отдельные модули приложения, предоставляя, таким образом, доступ к различным его областям. Также независимо от лицензирования вы можете включать или отключать ту или иную функциональность за счет использования конфигурационных ключей.

Обзор подсистемы контроля доступа

Подсистема контроля доступа Microsoft Dynamics AX состоит из трех уровней: аутентификация, авторизация и контроль доступа к данным. На рис. 11-1 представлено высокоуровневое описание архитектуры контроля доступа в Microsoft Dynamics AX. В следующих разделах каждый уровень описан более детально.

Аутентификация

Аутентификация – это процесс проверки подлинности учетных данных пользователя. В Microsoft Dynamics AX пользователи могут аутентифицироваться двумя способами. Первый – использование интегрированной аутентификации Windows для проверки подлинности учетных данных пользователей Active Directory. Это достигается за счет того, что пользователем Microsoft Dynamics AX делается либо отдельный пользователь Windows, либо целая группа Active Directory. После того как группа Active Directory будет добавлена в качестве пользователя в Microsoft Dynamics AX, любой пользователь, входящий в эту группу, сможет получить доступ к Microsoft Dynamics AX. Добавление групп Active Directory в качестве пользователя является новой возможностью Microsoft Dynamics AX 2012.

Второй способ аутентификации пользователя называется *гибкой аутентификацией* (flexible authentication), это также новая возможность Microsoft Dynamics AX 2012. За счет гибкой аутентификации пользователь может быть аутентифицирован для использования веб-клиента корпоративного портала Microsoft Dynamics AX, и при этом ему не потребуются учетные данные Active Directory.

Рис. 11–1. Высокоуровневое описание архитектуры контроля доступа в Microsoft Dynamics AX

Гибкая аутентификация использует аутентификацию на основе утверждений (claims-based authentication) для проверки подлинности пользователей корпоративного портала. За более детальной информацией обратитесь к официальному документу «Flexible Authentication in Microsoft Dynamics AX 2012» по адресу: *http://www.microsoft.com/en-us/download/details.aspx?id=29050*.

После того как пользователь подключится к Microsoft Dynamics AX, происходит его авторизация в системе. Эта тема рассмотрена далее.

Авторизация

Авторизация, также именуемая *управлением доступом,* определяет, разрешено ли пользователю осуществлять то или иное действие. В Microsoft Dynamics AX, как при доступе через Windows-клиента, так и в корпоративном портале, используются права доступа для контроля доступа к отдельным элементам приложения: меню, пунктам меню, кнопкам, отчетам, сервисным операциям, пунктам меню, содержащим web URL, элементам управления веб-страниц и отдельным полям. В Microsoft Dynamics AX 2012 новая модель контроля доступа следует принципу контроля на основе ролей. Эта модель является иерархической: каждый элемент в иерархии представляет тот или иной уровень детализации, начиная с разрешений, находящихся на самом нижнем уровне.

- *Разрешения* представляют доступ к отдельным защищаемым объектам, таким как пункты меню и таблицы.
- *Привилегии* состоят из разрешений и представляют доступ к отдельным задачам, таким как отмена платежей или работа с депозитами.
- *Обязанности (duties)* состоят из привилегий и представляют отдельные участки бизнес-процесса, такие как ввод банковских проводок.
- *Роли* состоят из обязанностей и иногда привилегий и определяют уровень доступа пользователя к Microsoft Dynamics AX. Эти роли соответствуют ролям внутри организации, таким как бухгалтер или менеджер по персоналу.

На рис. 11-2 представлены элементы контроля доступа, основанного на ролях, а также взаимосвязи этих элементов контроля доступа.

В следующем разделе элементы модели контроля доступа описаны более подробно.

Разрешения

В модели контроля доступа Microsoft Dynamics AX разрешения группируют защищаемые объекты и уровни доступа, которые необходимы для выполнения той или иной функции. К ним могут относиться любые таблицы, поля, формы или выполняемые на сервере статические методы, доступ к которым осуществляется через точку входа. Пункты меню, элементы веб-контента и сервисные операции собирательно называются *точками входа*. Через точки входа осуществляется доступ к каждой функции в Microsoft Dynamics AX, такой как форма или сервис.

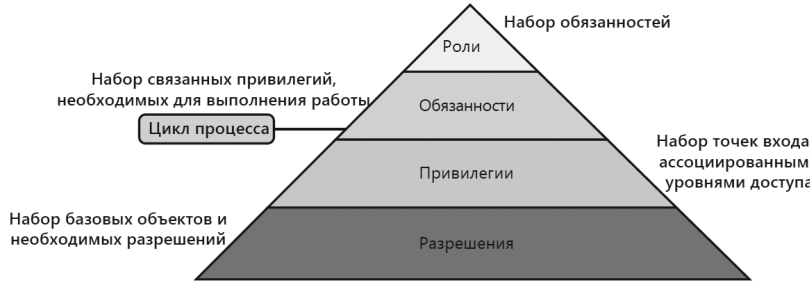

Рис. 11–2. Элементы контроля доступа, основанного на ролях, и взаимосвязи этих элементов контроля доступа

Создавать или изменять разрешения могут только разработчики. Как это делать, подробно объясняется в разделе «Разработка артефактов контроля доступа» далее в этой главе.

Привилегии

Привилегия определяет уровень доступа, который необходим для осуществления работы, решения проблемы или выполнения задания. Привилегии могут назначаться напрямую ролям, однако для упрощения поддержки и обслуживания системы ролям рекомендуется назначать лишь обязанности.

Привилегия содержит разрешения для отдельных объектов приложения, таких как элементы пользовательского интерфейса и таблицы. Например, привилегия *Отмена платежей* содержит разрешения на пункты меню, поля и таблицы, которые необходимы для выполнения отмены платежей.

Привилегии предоставляются по умолчанию для всех функциональных возможностей, реализованных в Microsoft Dynamics AX. Системный администратор может изменить разрешения, которые связаны с привилегией, либо создать новые привилегии.

Обязанности

Обязанность – это группа привилегий или задач, которая соответствует части бизнес-процесса. Системный администратор назначает обязанности ролям безопасности. Обязанность может быть назначена более чем одной роли.

В модели контроля доступа Microsoft Dynamics AX обязанности содержат привилегии. Например, обязанность *Ввод банковских проводок*

содержит привилегии *Создание депозитарных расписок* и *Отмена платежей*. Хотя той или иной роли безопасности могут назначаться и обязанности, и привилегии, рекомендуется использовать именно обязанности для предоставления доступа к Microsoft Dynamics AX. За счет этого вы сможете использовать функционал разделения обязанностей, описанный в следующем подразделе.

Из соображений безопасности или в соответствии с корпоративной политикой может потребоваться, чтобы определенные задачи выполнялись различными пользователями. Например, для организации может быть нежелательно, чтобы один и тот же человек выполнял как подтверждение приемки товара, так и обработку платежей поставщикам. Этот подход называется «разделением обязанностей». Он помогает организациям уменьшить риск воровства, а также выявлять ошибки или отклонения от обычного порядка ведения дел. За счет разделения обязанностей организация может лучше соответствовать регулирующему законодательству. В Microsoft Dynamics AX 2012 разделение обязанностей позволяет системному администратору указать, какие обязанности всегда должны быть разделены и не могут совмещаться тем или иным пользователем.

В Microsoft Dynamics AX есть преднастроенные обязанности, но системный администратор может изменить привилегии, которые связаны с той или иной обязанностью, или создать новые обязанности. За более детальной информацией обратитесь к разделу «Настройка правила разделения обязанностей» далее в этой главе.

Циклы процесса

Бизнес-процесс является согласованным набором видов деятельности, в котором один или более участников потребляют, производят или используют экономические ресурсы для достижения организационных целей. В контексте модели контроля доступа бизнес-процессы называют *циклами процесса*. Чтобы помочь системным администраторам выявить обязанности, которые должны быть назначены ролям, эти обязанности сгруппированы по бизнес-процессам, к которым они относятся. К примеру, в цикле процесса учета вы можете найти такие обязанности, как *Ведение бухгалтерских счетов* и *Ведение банковских проводок*. Циклы процесса используются только для той или иной организации.

Роли безопасности

Microsoft Dynamics AX 2012 использует контроль доступа на основе ролей. Иными словами, доступ предоставляется не отдельным пользователям, а

ролям безопасности. Назначенные пользователю роли безопасности определяют обязанности, которые пользователь может выполнять, и части пользовательского интерфейса, которые пользователь может видеть.

Microsoft Dynamics AX 2012 предоставляет возможность отслеживания привязанных к датам данных за счет использования таблиц с историей состояния. Для таких таблиц системный администратор может указать, какой у роли пользователя будет уровень доступа к записям, относящимся к текущему, прошлому и будущему периодам.

Управляя доступом посредством ролей безопасности, системные администраторы экономят свое время, потому что им не приходится разграничивать доступ отдельно для каждого пользователя. Роли безопасности определяются сразу для всех организаций. Назначить пользователю роль безопасности можно несколькими способами. Один из них – непосредственное назначение роли безопасности пользователю. Другой способ – назначение роли группе пользователей Active Directory, за счет чего эта роль назначается всем входящим в группу пользователям. Помимо этого, роли безопасности могут назначаться пользователям автоматически на основании бизнес-данных. К примеру, системный администратор может настроить правило, согласно которому роль безопасности связывается с определенной должностью в настройках модуля управления персоналом. Каждый раз, когда пользователю в системе назначается эта должность, ему также автоматически добавляется соответствующая роль безопасности. Этот функционал называется *динамическим назначением ролей*. Как правило, роли безопасности пользователям назначает системный администратор.

Роли безопасности могут быть организованы в иерархию, чтобы каждую роль безопасности можно было определить как комбинацию других ролей. К примеру, роль безопасности *Менеджер по продажам* может быть определена как комбинация ролей *Менеджер* и *Продавец*. Вместо настройки с нуля каждой роли иерархически организованные роли безопасности могут наследовать права доступа от других ролей и повторно использовать их настройки.

Для предоставления доступа к программе в модели безопасности Microsoft Dynamics AX используются обязанности и привилегии. К примеру, роли менеджера по продажам могут быть назначены обязанности *Поддержание политик по выручке* и *Проверка заказов на продажу*.

По умолчанию предоставляются простые роли безопасности, и вся функциональность Microsoft Dynamics AX привязана как минимум к од-

ной из ролей безопасности, идущих в стандартной поставке. Системный администратор может назначать пользователям идущие в стандартной поставке роли безопасности, изменять эти роли под нужды бизнеса или же создавать новые роли.

Примечание. Роли безопасности, идущие в стандартной поставке, не соответствуют ролевым центрам, которые являются домашними страницами по умолчанию, предоставляющими обзор информации, относящейся к работе пользователя, такой как список рабочих заданий, мероприятия, часто используемые ссылки и ключевые данные бизнес-аналитики.

Контроль доступа к данным

Как упоминалось ранее, в Microsoft Dynamics AX 2012 появилась новая расширяемая инфраструктура контроля доступа к данным (extensible data security framework, XDS), с помощью которой вы можете управлять доступом к транзакционным данным за счет привязки к ролям безопасности политик контроля доступа к данным. Эти политики могут ограничивать доступ к данным на основе их даты вступления в силу или же на основе пользовательских данных, таких как территория сбыта или организация, к которой относится пользователь.

Примечание. Контроль доступа к данным отделен от контроля доступа к функционалу, что достигается за счет использования контроля доступа на базе ролей. В дополнение к XDS, для ограничения доступа к данным вы можете использовать настройки безопасности на уровне записей (RLS), которые основаны на запросах. Однако, поскольку в будущих версиях Microsoft Dynamics AX функционал RLS будет удален как устаревший, рекомендуется вместо него использовать XDS.

Кроме того, в Microsoft Dynamics AX для защиты данных есть инфраструктура прав доступа к таблицам. Эта инфраструктура позволяет принудительно проверять права доступа к данным на сервере приложений (AOS). Когда пользователь пытается получить доступ к данным таблиц, защищенным инфраструктурой проверки прав доступа к таблицам, то выполняются явные проверки авторизации.

Разработка артефактов контроля доступа

Доступ к защищенным объектам в Microsoft Dynamics AX контролируется с помощью различных артефактов контроля доступа, таких как разрешения, привилегии, обязанности, роли и политики. Создавать эти артефакты и управлять ими вы можете с помощью AOT, как показано на рис. 11-3.

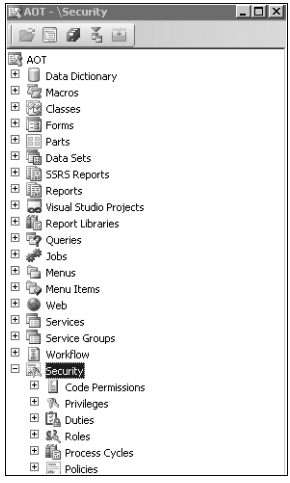

Рис. 11–3. Артефакты контроля доступа в AOT

Установка разрешений для формы

Безопасность строится с самых низов, начиная с уровня формы. Первым шагом является обеспечение контроля доступа к данным на форме. Когда вы сохраняете форму в AOT, Microsoft Dynamics AX автоматически выводит все таблицы и другие элементы, к которым форма получает доступ (то есть автоматически узнает о них). Эта функциональность называется *автовыведением* (*auto-inference*). Автовыведение упрощает настройку разрешений для таблиц. В зависимости от таблиц, используемых на форме, для нее автоматически устанавливаются разрешения на создание, чтение, обновление и удаление (create, read, update, delete, CRUD). Система автоматически добавляет или обновляет подузлы *Read*, *Update*, *Create* и *Delete* в AOT (в узле AOT\Forms\<*НазваниеФормы*>\Permissions).

На рис. 11-4 показан набор разрешений для формы *AgreementClassification*.

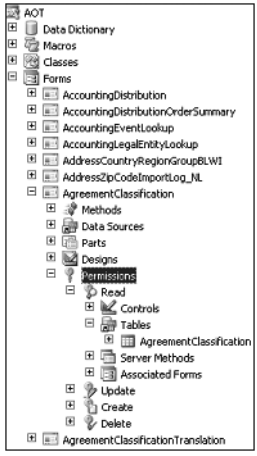

Рис. 11–4. Разрешения на чтение для формы *AgreementClassification*

Хотя разрешения для источников данных устанавливаются автоматически за счет функционала автовыведения, вы также можете установить разрешения для источника данных вручную. К примеру, в узле разрешений на чтение (Read), показанном на рис. 11-4, свойства таблицы *AgreementClassification* установлены с помощью автовыведения (см. рис. 11-5).

Table AgreementClassification

Properties | Categories

Table	AgreementClassification
EffectiveAccess	Read
DefaultAccess	Read
SystemManaged	Yes
ManagedBy	

Рис. 11–5. Свойства таблицы *AgreementClassification*, установленные с помощью автовыведения

Свойство *SystemManaged* установлено в *Yes*. Однако вы можете изменить значение свойства *EffectiveAccess* на что-либо, отличное от *Read*. В этом случае значение свойства *SystemManaged* изменится на *No*. Это будет указывать инфраструктуре контроля доступа, что вы решили вручную изменить значение, которое было установлено за счет автовыведения (см. рис. 11-6).

Table AgreementClassification

Properties | Categories

Table	AgreementClassification
EffectiveAccess	Create
DefaultAccess	Read
SystemManaged	No
ManagedBy	

Рис. 11–6. Свойства таблицы *AgreementClassification*, установленные вручную

Пока что в этом разделе обсуждались отдельные права доступа к элементам в узле *Tables*. Но вы также можете устанавливать разрешения для других узлов, таких как *Controls*, *Server Methods* и *Associated Forms*. Заметьте, что аналогично установке разрешений для форм вы также можете устанавливать разрешения на чтение и запись данных для элементов в узле *Permissions* для некоторых других типов объектов AOT, включая следующие:

- Forms\<*НазваниеФормы*>;
- Parts\Info Parts\<*НазваниеInfoPart*>;
- Reports\<*НазваниеОтчета*>;
- Web\Web Files\Web Controls\<*НазваниеWebЭлементаУправления*>;
- Services\<*ServiceName*>\Operations\<*НазваниеОперации*>.

Настройки в узле *Associated Forms* используются во время выполнения тогда, когда на родительской форме (*AgreementClassification* в данном случае) есть кнопка, открывающая другую форму. В таких случаях следует добавить разрешения, чтобы связанная форма была доступна пользователям родительской формы, для чего добавьте ссылку на связанную форму в узел *Associated Forms*. Когда у пользователя есть доступ к форме, то по умолчанию у него есть доступ ко всем элементам управления на ней. Вы можете переопределить эти настройки по умолчанию, добавив разрешения для отдельных элементов управления. Это можно сделать в узле *Controls*.

Установка разрешений для серверных методов

Если серверный метод помечен атрибутом *SysEntryPointAttribute*, то пользователям должен быть явно предоставлен доступ к этому методу. Если такой серверный метод вызывается из формы, то вы можете разграничить доступ к нему за счет добавления этого метода в узел *Server Methods* и явного указания разрешений для его вызова. Любая роль, предоставляющая доступ к форме через соответствующее разрешение (в данном случае на чтение [read]) также предоставляет разрешение на вызов серверного метода.

Установка разрешений для элементов управления

Когда вы разрабатываете форму, Microsoft Dynamics AX предоставляет возможность добавлять элементы управления на форму как объекты, защищаемые механизмом контроля доступа; элементы управления при этом

могут быть как привязаны к источнику данных формы, так и не привязаны. Контроль доступа ко всем элементам управления с привязкой к данным (data-bound) осуществляется автоматически, в то время как доступ к элементам управления без привязки к данным (unbound) можно осуществлять из кода. В случае с элементами управления без привязки к данным, таким как кнопка, использующая пункт меню, контроль доступа связан с объектом, на который ссылается такой элемент управления, а видимость управляется разрешениями для соответствующего объекта.

Создание привилегий

Следующим шагом после установки разрешений является создание привилегий. Как упоминалось ранее, привилегия – это набор разрешений, который предоставляет доступ к защищаемым объектам. За счет использования автоматически выведенных разрешений для таблиц и защиты пунктов меню с помощью привилегий вы можете контролировать доступ к данным на форме. В следующем примере (рис. 11-7) точка входа для формы связывается с соответствующими разрешениями.

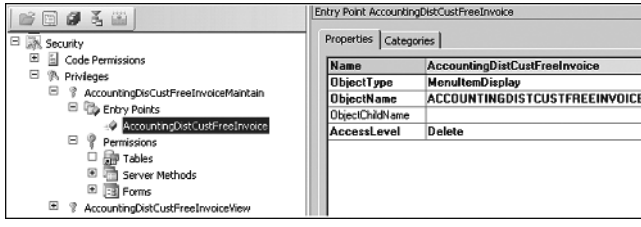

Рис. 11–7. Связывание формы с разрешениями

В этом примере привилегия *AccountDistCustFreeInvoiceMaintain* содержит точку входа *AccountingDistCustFreeInvoice* – это пункт меню, который, в свою очередь, ссылается на форму. Обратите внимание, что значение свойства *AccessLevel* установлено в *Delete*. Это подразумевает, что, когда пользователь получает доступ к форме через этот конкретный пункт меню, инфраструктура контроля доступа Microsoft Dynamics AX будет просматривать содержимое узла *Permissions\Delete* этой формы и предоставит доступ к таблицам, которые перечислены в этом узле. Этот пример показывает, как система увязывает между собой привилегии, точки входа и разрешения для определения уровня доступа, который должен быть у пользователя, если у него есть доступ через роль безопасности к соответствующей привилегии.

Пункт меню предоставляет точку входа для открытия формы. Свойства контроля доступа в пункте меню управляют тем, какие наборы разрешений из соответствующей формы будут доступны для выбора, когда пункт меню будет связан с привилегиями. У каждого пункта меню есть такие свойства контроля доступа:

- *ReadPermissions;*
- *UpdatePermissions;*
- *CreatePermissions;*
- *CorrectPermissions;*
- *DeletePermissions.*

Эти свойства соответствуют узлам в AOT\Forms\<*НазваниеФормы*>\Permissions. К примеру, свойство *UpdatePermissions* соответствует узлу AOT\Forms\<*НазваниеФормы*>\Permissions\Update. В табл. 11-1 описываются значения этих свойств.

Табл. 11–1. Значения свойств для создания, обновления, чтения и удаления (create, update, read, delete)

Значение свойства	Описание
Auto	Значение по умолчанию. *Auto* означает, что соответствующий набор разрешений формы будет доступен для выбора в качестве привилегий для этого пункта меню. Привилегии будут выбраны из соответствующего узла привилегий этого пункта меню, который будет находиться в узле *Entry Points*. Путь к узлу привилегий для этого пункта меню – AOT\Security\Privileges*МояПривилегия*\Entry Points*МойПунктМеню*. К примеру, если свойство *UpdatePermissions* установлено в *Auto*, то для выбора в привилегиях в узле AOT\Security будет доступен набор разрешений в узле *МояФорма*\Permissions\Update
No	Противоположность *Auto*. Соответствующий набор разрешений не будет доступен для выбора в качестве привилегии в узле привилегий для этого пункта меню, который будет находиться в узле *Entry Points*

Например, если свойство *ReadPermisssions* пункта меню установлено в *No*, то этот пункт меню не будет задействовать свойство *ReadPermissions* той формы, на которую он ссылается. Вы можете использовать этот под-

ход, чтобы добавить разрешение для пункта меню, не затрагивая разрешения для того защищаемого объекта, который доступен через этот пункт меню. Таким образом, можно ограничить разрешения, которые системный администратор выдает для пункта меню, добавляемого в узел *Entry Points* привилегии.

В некоторых случаях пункт меню может ссылаться напрямую на класс или отчет – тогда вам придется ссылаться на класс, который сам по себе не связан ни с какими разрешениями. В этой ситуации потребуется использовать разрешение доступа к коду (code permission). *Разрешение доступа к коду* – это группа разрешений, которые связаны с пунктом меню или с сервисной операцией. Если вы хотите напрямую запускать какой-либо код через пункт меню, то должны установить для него разрешения доступа к коду (они также представлены в виде узлов AOT). Когда роль безопасности предоставляет доступ к какому-либо пункту меню, то у этой роли также есть доступ другим элементам AOT, которые перечислены в разрешении доступа к коду для этого пункта меню. Уровень доступа при этом контролируется разрешениями, установленными в узле *Code Permissions*.

Microsoft Dynamics AX использует концепцию объединения разрешений. Если для одного и того же объекта указано несколько различных разрешений через разные привилегии и роли, то уровень доступа к этому объекту будет являться результатом объединения этих разрешений. Например, если одна привилегия предоставляет к таблице доступ на чтение, а другая привилегия к той же таблице предоставляет полный доступ, и обе эти привилегии принадлежат к определенной роли безопасности, то у пользователя, которому будет назначена эта роль безопасности, будет полный доступ к соответствующей таблице.

Назначение привилегий и обязанностей ролям безопасности

После того как вы сформировали разрешения для различных защищаемых объектов, следует предоставить доступ к этим объектам через роли безопасности. Первым шагом при этом является создание привилегий, описанное в предыдущем разделе. Затем вы можете включить эти привилегии в обязанности или же напрямую назначить их ролям безопасности. На рис. 11-8 привилегия *AccountingDisCustFreeInvoiceMaintain* содержит точку входа *AccountingDisCustFreeInvoiceMaintain*.

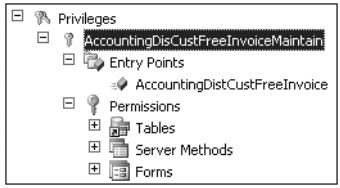

Рис. 11–8. Привилегия, содержащая точку входа

Точка доступа связана с уровнем доступа, указанным в ее свойствах (рис. 11-9). Обратите внимание, что в данном случае уровень доступа установлен в *Delete* (то есть полный доступ). Это подразумевает, что когда пользователь осуществляет доступ к точке входа, система будет просматривать узел *Permissions\Delete* для формы, которая запускается этой точкой входа.

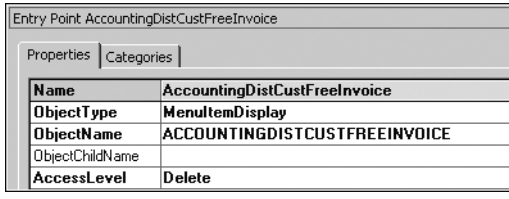

Рис. 11–9. Свойства точки входа

Назначение привилегии той или иной роли безопасности не напрямую, а через обязанность, не является обязательным требованием, однако такой способ позволит системным администраторам управлять привилегиями на более высоком уровне абстракции и использовать механизм контроля правил разделения обязанностей, чтобы соблюсти соответствующие требования по разделению обязанностей. На рис. 11-10 обязанность *CustInvoiceCustomerInvoiceTransMaintain* содержит привилегию *AccountingDisCustFreeInvoiceMaintain*.

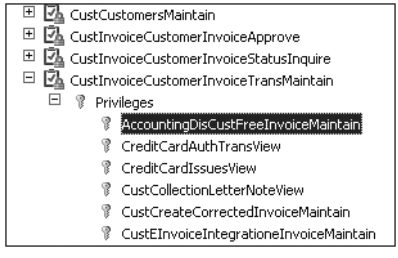

Рис. 11–10. Обязанность, содержащая привилегии

Продолжая рассмотрение этого примера, обратите внимание, как на рис. 11-11 обязанность *CustInvoiceCustomerInvoiceTransMaintain* представлена в рамках роли *CustInvoiceAccountsReceivableClerk*.

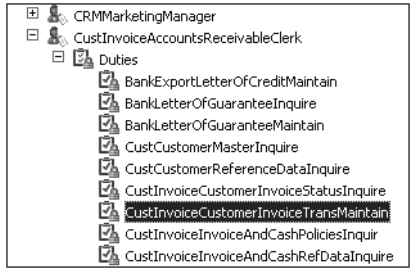

Рис. 11–11. Обязанности в рамках роли безопасности

Примечание. Более подробную информацию о контроле доступа в можете найти в разделе «Role-based security in the AOT for Developers» по адресу: *http://msdn.microsoft.com/en-us/library/gg847971*.

Использование таблиц со временем действия данных

Таблица со временем действия данных (valid time state table) помогает упростить поддержку данных, для которых необходимо отслеживать изменения в разрезе временных интервалов. Например, процентная ставка по займу может быть 5% для первого года выплат и 6% для второго года. В течение второго года вам все еще может быть необходимо знать, что в предыдущий год ставка составляла 5%.

Чтобы включить для таблицы отслеживание времени действия данных, установите свойство таблицы *ValidTimeStateFieldType* в AOT. После установки этого свойства система автоматически добавляет поля *ValidFrom* и *ValidTo*, в которых отслеживается диапазон дат для каждой записи. Система гарантирует поддержание корректности значений даты либо даты и времени в этих полях за счет автоматического предотвращения пересечений диапазонов дат. Данные, отслеживаемые в таблицах такого типа, называются *данными с датой вступления в силу* (*date effective)*.

Доступом к данным с датой вступления в силу управляют свойства роли безопасности. В AOT вы можете установить свойства *PastDataAccess*, *CurrentDataAccess* и *FutureDataAccess*. По умолчанию они установлены в *Delete* (полный доступ) – фактически это означает, что данные в таблицах не имеют даты вступления в силу. Однако если установить одно из этих

свойство в значение, отличное от *Delete*, то для таблиц, защищаемых ролью безопасности, оно будет указывать уровень доступа к данным, имеющим дату вступления в силу. Например, если обычный уровень доступа к таблице в данной роли безопасности – на изменение, а вы устанавливаете значение свойства *PastDataAccess* во *View*, то пользователь сможет изменять данные текущего и будущего периодов, но данные прошлых периодов сможет лишь просматривать.

Проверка артефактов контроля доступа

После настройки контроля доступа к данным вам, вероятно, захочется проверить, что все изменения реализованы корректно. Процесс тестирования состоит из следующих шагов.

1. Создание пользователей.
2. Назначение пользователям роли безопасности.
3. Настройка правила разделения обязанностей.

После выполнения этих шагов запустите клиента Microsoft Dynamics AX под тестовым пользователем, которому назначена подходящая роль (или роли) безопасности, и убедитесь, что контроль доступа к функционалу работает так, как задумывалось.

Создание пользователей

Пользователи Microsoft Dynamics AX – это либо сотрудники вашей организации, либо внешние клиенты и поставщики, которым требуется доступ к Microsoft Dynamics AX для выполнения их работы. Любой человек, которому необходим доступ в систему Microsoft Dynamics AX, должен быть добавлен в список пользователей Microsoft Dynamics AX на форме Администрирование системы > Общие > Пользователи > Пользователи.

Помимо прочих настроек на этой форме есть поле под названием *Тип счета*. Вы должны выбрать, будет ли пользователь или группа пользователей аутентифицированы средствами Active Directory либо средствами провайдера проверки подлинности на основе утверждений (claims-based authentication). Для Active Directory можно выбрать между добавлением в качестве пользователя Microsoft Dynamics AX отдельного пользователя Active Directory или же группы пользователей Active Directory.

Назначение пользователям роли безопасности

После создания пользователя в системе, ему назначается роль безопасности – либо вручную, либо автоматически. Вы можете настроить правила для автоматического назначения ролей, чтобы гарантировать, что принадлежность к той или иной роли основывается на актуальных бизнес-данных. Если вы используете автоматическое назначение ролей, то разрешения автоматически обновляются при изменении должностей сотрудников в организации. Правила автоматического назначения ролей безопасности применяются периодически через определенный интервал времени за счет использования инфраструктуры пакетных заданий. В рамках настройки правила вы выбираете запрос из AOT, на основании которого будет применяться это правило. Более подробную информацию вы можете найти в главе 18.

Если принадлежность к той или иной роли не может быть привязана к данным Microsoft Dynamics AX, то вы можете назначить роль вручную, например, в случае, если определенный сотрудник уходит в отпуск, а его обязанности временно должен выполнять другой сотрудник. Если системный администратор вручную назначил определенные роли безопасности пользователям, то и удалять их привязку к этим ролям он также должен вручную. С помощью правил автоматического назначения ролей эти назначения удалены не будут.

Настройка правила разделения обязанностей

Как упоминалось ранее, законодательное регулирование или политики безопасности могут требовать, чтобы определенные задачи выполнялись разными людьми. В Microsoft Dynamics AX, когда две обязанности в рамках одной роли конфликтуют или когда пользователю назначаются две роли, содержащие конфликтующие обязанности, выводится информация о таком конфликте. Вы должны подтвердить или отменить каждое назначение ролей, приводящее к нарушению правил разделения обязанностей. Более подробную информацию вы можете найти в разделе «Identify and resolve conflicts in segregation of duties» по адресу: *http://technet.microsoft.com/en-us/library/hh556858.aspx.*

Создание политик Extensible Data Security

В любой компании из соображений конфиденциальности, для соблюдения юридических требований или внутренних политик, определенным

пользователям может быть запрещен доступ к той или иной деликатной информации. В Microsoft Dynamics AX 2012 авторизация для доступа к деликатной информации осуществляется с помощью XDS.

Используя XDS, вы можете защитить данные в таблицах таким образом, что пользователи смогут получить доступ лишь к подмножеству записей таблицы, разрешенному той или иной политикой. Ниже приведены примеры типовых сценариев использования XDS.

- Позволить менеджерам по продажам видеть только тех клиентов, которых они обслуживают.
- Запретить для определенной роли безопасности видеть финансовые данные на формах или в отчетах.
- Запретить для определенной роли безопасности видеть подробные сведения о счетах или определенные коды счетов.

XDS является развитием безопасности на уровне записей (RLS), которая была доступна в более ранних версиях Microsoft Dynamics AX.

Политики контроля доступа к данным применяются на уровне сервера. Это означает, что настроенные политики XDS будут применяться независимо от того, осуществляется ли доступ к данным через формы Windows-клиента Microsoft Dynamics AX, веб-страницы Корпоративного портала, отчеты Microsoft SQL Server Reporting Services (SSRS) или же сервисы .NET. Кроме того, за счет использования новой инфраструктуры вы можете создать политики контроля доступа к данным, которые основаны на данных, содержащихся в иной таблице, нежели та, к которой они применяются.

Концепции политик контроля доступа к данным

Прежде чем приступить к разработке политики контроля доступа к данным, вам следует познакомиться с несколькими концепциями, такими как ограниченные таблицы, основные таблицы, запросы политик и контекст. В этом разделе приводятся краткие описания этих понятий; в последующих разделах они используются, чтобы показать, как эти концепции взаимодействуют для предоставления богатых возможностей инфраструктуры политик.

- *Ограниченная таблица (constrained table)* – это таблица (или таблицы) в политике контроля доступа, данные которой фильтруются или защищаются на основе связанного с политикой запроса. К примеру, в политике, которая защищает все заказы на продажу на основании группы клиентов, ограниченной таблицей будет SalesTable. Ограниченные таблицы в политике всегда явно связаны с основной таблицей.
- *Основная таблица (primary table)* используется для защиты данных в связанной ограниченной таблице. К примеру, в политике, которая защищает все заказы на продажу на основании группы клиентов, основной таблицей будет CustTable. Основная таблица одновременно может быть и ограниченной таблицей.
- *Запрос политики* используется для защиты ограниченных таблиц, указанных в политике XDS. Этот запрос возвращает данные из основной таблицы, которые затем используются для защиты содержимого ограниченной таблицы.
- *Контекст политики* – это некоторая информация, управляющая тем, при каких обстоятельствах данная политика применима. Если контекст не задан, то политика, даже если она активна, не будет применяться. Контексты политик могут быть двух типов: контексты роли и контексты приложения. *Контекст роли (role context)* позволяет применять политику в зависимости от роли или ролей, назначенных пользователю. *Контекст приложения (application context)* позволяет применять политику в зависимости от информации, установленной средствами приложения.

Разработка политики XDS

Разработка политики XDS включает следующие шаги.

1. Настройка запроса к основной таблице.
2. Создание элемента AOT для политики XDS.
3. Добавление ограниченных таблиц и представлений.
4. Настройка контекста политики.

На рис. 11-12 показано представление политики *VendProfileAccount* в AOT. Политики безопасности располагаются в узле *Security\Policies*.

Рис. 11–12. Политика безопасности в AOT

На рис. 11-13 показаны свойства этой политики безопасности.

Security Policy VendProfileAccount

Properties | Categories

Name	**VendProfileAccount**
Label	**Security policy for external vendors**
PrimaryTable	**VendTable**
Query	**VendProfileAccountPolicy**
PolicyGroup	**Vendor Self Service**
ConstrainedTable	**Yes**
Enabled	**Yes**
HelpText	
Operation	Select
ContextType	**RoleProperty**
ContextString	**PolicyForVendorRoles**
RoleName	

Рис. 11–13. Свойства политики безопасности

Обратите внимание, что на рис. 11-13 установлены следующие свойства политики.

- Свойство *PrimaryTable* установлено в *VendTable*.
- Свойство *Query* установлено в *VendProfileAccountPolicy*. Запрос политики определен в AOT и может использовать всю функциональность, предоставляемую такими запросами. При создании запроса основная таблица должна быть первым источником данных; в случае необходимости можно добавить дополнительные источники данных. В этом примере дополнительные источники данных определяются связями и отношениями между таблицами модуля поставщиков.

- Свойство *Operation* установлено в *Select*. Запрос политики может быть добавлен в выражение *WHERE* (или выражение *ON*) для всех операторов *SELECT*, *UPDATE*, *DELETE* и *INSERT*, включающих ограниченные таблицы. В данном случае политика будет применяться только к операторам *SELECT*.
- Свойство *PolicyGroup* установлено в *Vendor Self Service*. Это свойство используется для обозначения групп связанных политик, во время выполнения оно никак не задействуется.
- Свойство *ConstrainedTable* установлено в *Yes*, указывая, что основная таблица будет защищена с помощью этой политики. Иными словами, таблица, данные которой фильтруются или защищаются, является той же самой таблицей, что указана в свойстве *PrimaryTable*. Если это свойство установлено в *No*, то политика не будет применяться к основной таблице.
- Свойство *Enabled* установлено в *Yes*, указывая, что политика будет применяться во время выполнения.
- Свойство *ContextType* установлено в *RoleProperty*, указывая, что политика должна применяться лишь в случае, если пользователю назначена одна из множества ролей, у которых свойство *ContextString* имеет то же значение. В данном примере свойство *ContextString* установлено в *PolicyForVendorRoles*. Если у каких-либо ролей в AOT свойство *ContextString* также установлено в *PolicyForVendorRoles*, то политика будет применяться для пользователей, которым назначены эти роли. Помимо значения *RoleProperty*, свойство *ContextType* может быть установлено в *ContextString* и *RoleName*. *ContextString* указывает, что вам нужно задать значение свойства *ContextString,* при этом политика безопасности будет использовать определенный контекст приложения. Свойство *RoleName* указывает, что политика безопасности будет применяться только к пользователям, которым назначена роль, заданная в свойстве *RoleName*.

Сложные и нормализованные схемы данных могут привести к использованию запросов с многочисленными объединениями таблиц, что может негативно сказаться на производительности. Однако подавляющая часть запросов политик выбирает статические данные, такие как коды юридических лиц, доступных пользователю, и коды подразделений, к которым он относится. XDS предоставляет возможность снизить частоту обращений

к таким статическим данным (при этом частота обращений может варьироваться от одного раза на каждый запрос к таблице до одного раза за все время жизни клиентской сессии) и повторно использовать результаты выборки при последующем применении политики. Этот механизм называется «конструктивами XDS».

Конструктивы XDS (extensible data security constructs) – это таблицы типа **TempDB, которые заполняются в соответствии со значением пере**числения *RefreshFrequency* для соответствующей таблицы (*PerSession* или *PerInvocation*). Они находятся в AOT, в узле *Data Dictionary\Tables*. На рис. 11-14 показан пример конструктива XDS.

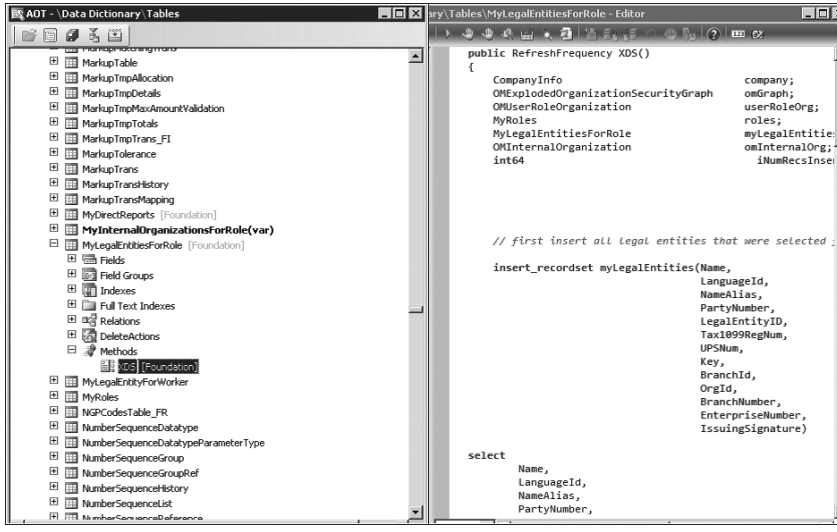

Рис. 11–14. Конструктив XDS

Временная таблица, используемая для конструктива XDS, заполняется с помощью табличного метода с названием *XDS*. В этом методе вы можете написать на X++ бизнес-логику заполнения временной таблицы. На рис. 11-14 *MyLegalEntitiesForRole* – это конструктив XDS, который заполняется методом XDS. **Метод заполняет таблицу кодами юридических лиц, к ко**торым у текущего пользователя есть доступ в контексте роли. Примером запроса политики, использующего конструктив *MyLegalEntitiesForRole,* является запрос *HcmXdsApplicantLegalEntity*. Он включает объединение четырех источников данных, последний из которых – конструктив *MyLega-*

lEntitiesforRole, инкапсулирующий несколько других объединений таблиц. Если метод XDS возвращает значение частоты обновления *PerSession*, то во время выполнения таблица в TempDB будет заполняться при ее первом использовании в любом запросе. Если бы конструктивы XDS не использовались, то каждый запрос с применением политики включал бы объединение еще четырех таблиц — это существенная дополнительная нагрузка с точки зрения производительности.

В этом сценарии конструктив XDS преобразует запрос политики с семью или более объединениями таблиц в запрос политики с четырьмя объединениями, что дает существенный выигрыш в производительности.

Отладка политик XDS

Одна из часто встречающихся проблем, о которых сообщается при использовании на проекте политик XDS, связана с тем, что выборка из ограниченной таблицы возвращает иное число записей, нежели ожидалось. XDS предоставляет отладочный механизм для решения подобных проблем. Для оператора *select* в X++ был добавлен новый хинт *generateonly*, уведомляющий инфраструктуру доступа к данным о том, что нужно лишь сгенерировать запрос SQL, но не отправлять его на СУБД. Вы можете получить сгенерированный запрос с помощью простого вызова метода.

Следующий job выполняет оператор *select* по таблице SalesTable с хинтом *generateonly*. Затем он вызывает метод *getSQLStatement* на табличном буфере SalesTable и выводит результат с помощью метода *info*.

```
static void VerifySalesQuery(Args _args)
{
SalesTable salesTable;
XDSServices xdsServices = new XDSServices();
xdsServices.setXDSContext(1, '');
// только генерируем SQL-запрос
select generateonly forceLiterals CustAccount, DeliveryDate from salesTable;
// выводим SQL-запрос в infolog
info(salesTable.getSQLStatement());
xdsServices.setXDSContext(2, '');
}
```

XDS еще больше упрощает процесс отладки за счет того, что сохраняет запросы в читаемом виде. Этот и другие запросы к ограниченной таблице в политике могут быть получены с помощью следующего запроса Transact-SQL (T-SQL) к БД в среде разработки (AXBDEV в данном примере):

```
SELECT [PRIMARYTABLEAOTNAME], [QUERYOBJECTAOTNAME], [CONSTRAINEDTABLE],
[MODELEDQUERYDEBUGINFO], [CONTEXTTYPE], [CONTEXTSTRING], [ISENABLED],
[ISMODELED]
FROM [AXDBDEV].[dbo].[ModelSecPolRuntimeEx]
```

Результаты выполнения запроса показаны на рис. 11-15.

	QUERYOBJECTAOTNAME	CONSTRAINEDTABLE	MODELEDQUERYDEBUGINFO
1	VendProfileAccountPolicy	AssetBook	SELECT * FROM AssetBook(AssetBook_1) EXISTS JOIN 'x' FROM VendTable(VendTabl...
2	VendProfileAccountPolicy	AssetBookMerge	SELECT * FROM AssetBookMerge(AssetBookMerge_1) EXISTS JOIN 'x' FROM VendTa...
3	VendProfileAccountPolicy	AssetDepBook	SELECT * FROM AssetDepBook(AssetDepBook_1) EXISTS JOIN 'x' FROM VendTable(V...
4	VendProfileAccountPolicy	AssetTable	SELECT * FROM AssetTable(AssetTable_1) EXISTS JOIN 'x' FROM VendTable(VendTa...
5	VendProfileAccountPolicy	BankCentralBankPurpose	SELECT * FROM BankCentralBankPurpose(BankCentralBankPurpose_1) EXISTS JOIN '...
6	VendProfileAccountPolicy	BankChequeReprints	SELECT * FROM BankChequeReprints(BankChequeReprints_1) EXISTS JOIN 'x' FROM ...
7	VendProfileAccountPolicy	BankChequeTable	SELECT * FROM BankChequeTable(BankChequeTable_1) EXISTS JOIN 'x' FROM Vend...

Рис. 11–15. Результаты выполнения запроса к ограниченной таблице

Как видно на рис. 11-15, запрос, который будет добавлен к выражению *WHERE* любого запроса к таблице AssetBook, доступен для отладки. Кроме самого запроса, доступны и другие метаданные, такие как *LayerId*.

При разработке политик придерживайтесь следующих принципов.

- Следуйте стандартным рекомендациям для разработки эффективных запросов. К примеру, создавайте индексы по полям, входящим в условия объединения таблиц.
- По возможности сокращайте число объединений источников данных в запросе. Сложные и нормализованные схемы данных могут привести к использованию запросов с многочисленными объединениями таблиц. Старайтесь сокращать число объединений таблиц, используемых во время выполнения, для чего можно изменить схему данных или использовать шаблоны, такие как конструктивы XDS. Учтите, что при одновременном применении нескольких политик к одной таблице соответствующие условия фильтрации объединяются с помощью операторов *AND*.

Написание защищенного кода

В этом разделе описаны возможности Microsoft Dynamics AX по поддержке инициативы Trustworthy Computing, при этом основное внимание уделяется тому, как они влияют на написание защищенного кода. В разделе описана инфраструктура прав доступа к таблицам, контроль доступа к коду (code access security, CAS) и правила Best Practices, автоматическая проверка которых позволит убедиться, что в коде не допущены некоторые

наиболее часто встречающиеся просчеты, связанные с безопасностью и контролем доступа.

Инфраструктура прав доступа к таблицам

Инфраструктура прав доступа к таблицам обеспечивает контроль доступа к данным таблиц БД, доступным через AOT. Свойство таблицы *AOSAuthorization* (рис. 11-16) указывает, какие операции должны проходить через проверку авторизации, когда пользователь обращается к таблице.

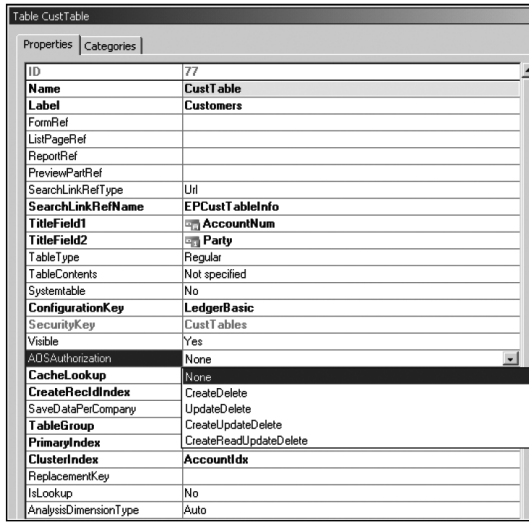

Рис. 11–16. Набор свойств таблицы

Свойство *AOSAuthorization* – это перечисление, в табл. 11-2 приведены его возможные значения.

Табл. 11–2. Значения свойства *AOSAuthorization*

Значение	Описание
None	На AOS не выполняются никакие проверки авторизации (значение по умолчанию)
CreateDelete	На AOS выполняются проверки авторизации операций создания и удаления записей
UpdateDelete	На AOS выполняются проверки авторизации операций обновления и удаления записей

Табл. 11–2. Значения свойства *AOSAuthorization (окончание)*

Значение	Описание
CreateUpdateDelete	На AOS выполняются проверки авторизации операций создания, обновления и удаления записей
CreateReadUpdateDelete	На AOS выполняются проверки авторизации всех операций манипуляции данными

В дополнение к свойству *AOSAuthorization* вы можете добавить дополнительные правила проверки с помощью следующих табличных методов:

- *aosValidateDelete;*
- *aosValidateInsert;*
- *aosValidateRead;*
- *aosValidateUpdate.*

Примечание. Эти методы влияют на производительность. При их использовании все операции с данными переводятся в режим обработки по одной записи за раз.

В Microsoft Dynamics AX 2012 также был введен новый класс для выполнения проверок авторизации. Используйте класс *SysEntryPointAttribute* для обозначения того, какие проверки авторизации должны выполняться для метода при его вызове на сервере. Когда вы помечаете метод этим атрибутом, то при выполнении метода класса на сервере осуществляется проверка авторизации. Вы можете дополнительно контролировать проверки с помощью параметра, передаваемого конструктору класса *SysEntryPointAttribute*, как описано в табл. 11-3.

Табл. 11–3. Параметры конструктора *SysEntryPointAttribute*

Настройка атрибута	Описание
[SysEntryPointAttribute(true)]	Указывает, что проверки авторизации должны выполняться для всех таблиц, к которым метод осуществляет доступ, даже если свойство *AOSAuthorization* для них установлено в *None*
[SysEntryPointAttribute(false)]	Указывает, что проверки авторизации не должны выполняться для таблиц, к которым метод осуществляет доступ

Microsoft Dynamics AX 2012 также предоставляет возможности для выполнения усечения данных на уровне сервера. Для таблиц, у которых свойство *AOSAuthorization* установлено в *CreateReadUpdateDelete*, можно установить свойство *AOSAuthorization* на отдельных полях в значение *Yes* или *No*. По умолчанию используется значение *No*, а значение *Yes* указывает, что проверки авторизации должны выполняться при операциях чтения и записи в поле. Если у пользователя нет доступа к тому или иному полю, то при значении *Yes* свойства *AOSAuthorization* для этого поля его значение не будет возвращено пользователю. Таким образом выполняется усечение данных на уровне сервера.

Контроль доступа к коду

Инфраструктура контроля доступа к коду (code access security, CAS) предоставляет методы защиты прикладных программных интерфейсов (API) от попыток их вызова сторонним кодом (имеющим происхождение не из AOT). Вы можете сделать тот или иной API более безопасным, реализовав наследника класса *CodeAccessPermission*. Класс, производный от *CodeAccessPermission*, с помощью проверки соответствующего разрешения определяет, можно ли доверять коду, вызывающему функцию API.

Чтобы защитить класс, который выполняется на сервере, выполните следующие шаги.

1. Создайте новый класс-наследник класса *CodeAccessPermission* либо используйте один из следующих существующих классов-наследников, которые уже есть в Microsoft Dynamics AX, и перейдите к шагу 6:
   - *ExecutePermission;*
   - *FileIOPermission;*
   - *InteropPermission;*
   - *RunAsPermission;*
   - *SkipAOSValidationPermission;*
   - *SqlDataDictionaryPermission;*
   - *SqlStatementExecutePermission;*
   - *SysDatabaseLogPermission.*
2. Создайте метод, возвращающий параметры класса.
3. Создайте конструктор со всеми параметрами класса, которые хранят данные о разрешении.

4. Для определения того, существует ли разрешение, необходимое для вызова защищаемого API, перекройте метод класса

   CodeAccessPermission.isSubsetOf, чтобы сравнивать производный класс разрешения с *CodeAccessPermission*. Следующий пример кода показывает, как перекрыть метод *CodeAccessPermission.isSubsetOf* для определения того, существуют ли в *_target* разрешения, хранящиеся в текущем объекте:

```
public boolean isSubsetOf(CodeAccessPermission _target)

{

    SysTestCodeAccessPermission sysTarget = _target;

    return this.handle() == _target.handle();

}
```

5. Перекройте метод *CodeAccessPermission.copy*, чтобы возвращать копию экземпляра класса, созданного на шаге 1. Это поможет предотвратить модификацию объекта класса перед передачей в защищаемую функцию API.
6. Вызовите метод *CodeAccessPermission.demand* перед выполнением функционала API, который вы защищаете. Этот метод проверяет стек вызовов, чтобы определить, было ли вызывающему коду предоставлено разрешение, необходимое для использования этого API.

Когда вы защищаете API описанным выше способом, то должны вызвать метод *assert* производного класса разрешений перед обращением к API. В противном случае будет выброшено исключение *Exception::CodeAccessSecurity*.

Правила Best Practices

Инструмент проверки правил Best Practices может помочь проверить код вашего приложения, чтобы убедиться, что он согласуется с инициативами Trustworthy Computing. Проверяемые правила, относящиеся к Trustworthy Computing, на форме параметров проверки Best Practices сгруппированы в Общие проверки\Trustworthy Computing, как показано на рис. 11-17. Форма параметров проверки Best Practices доступна в рабочей области разработки в меню Сервис > Параметры > Разработка > Best Practices.

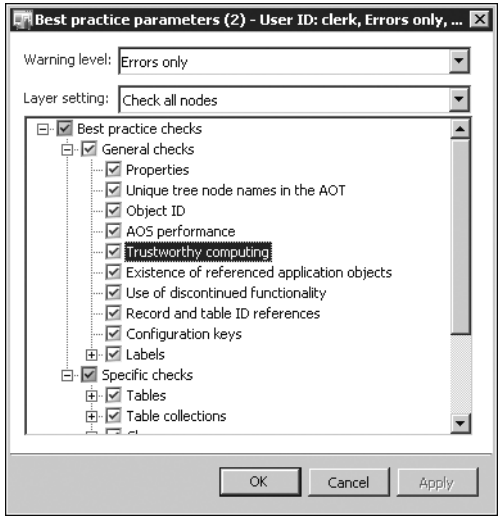

Рис. 11–17. Форма параметров проверки Best Practices с правилами Trustworthy Computing

Более подробную информацию об инструменте проверки Best Practices вы можете найти в главе 2.

Отладка прав доступа

Для помощи в отладке конструктивных элементов контроля доступа существуют пункты контекстного меню для некоторых узлов объектов AOT, связанных с контролем доступа, благодаря которым упрощается поиск объектов и ролей, связанных с определенным конструктивным элементом контроля доступа. В зависимости от того, на какой уровень в иерархии системы контроля доступа вы смотрите (рис. 11-2), у вас есть возможность просмотреть связанные элементы, находящиеся выше или ниже по иерархии. К примеру, для определенной обязанности вы можете увидеть все роли, в которые она входит, и все связанные привилегии и другие объекты контроля доступа, которые содержатся в этой обязанности. Эту информацию можно использовать для отладки проблем, связанных с уровнем доступа к различным защищаемым объектам.

Вот пример того, как можно использовать эти возможности для обязанности.

1. В AOT разверните узел Security\Duties.
2. Щелкните правой кнопкой мыши по обязанности и из контекстного меню выберите пункт Надстройки > Средства безопасности, затем

пункт Просмотр связанных объектов безопасности или пункт Просмотр связанных ролей безопасности.

3. Просмотрите путь к объектам, который будет отображен в открывшейся форме. На рис. 11-18 показан пример формы, отображаемой, когда для роли в AOT\Security\Roles выбирается пункт Просмотр связанных объектов безопасности.

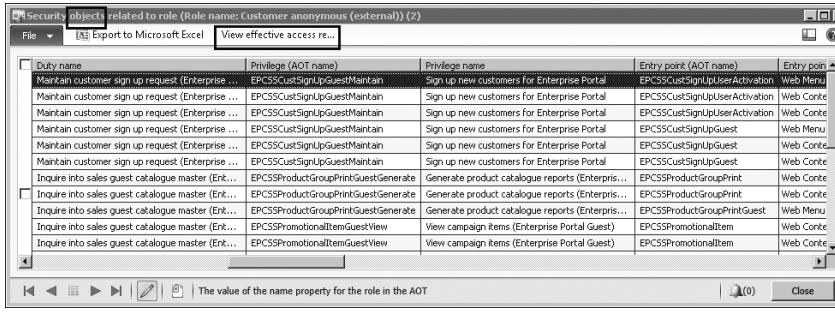

Рис. 11–18. Объекты контроля доступа для роли

Обратите внимание, что при просмотре связанных с ролью объектов контроля доступа у вас также есть возможность увидеть эффективный уровень доступа (как показано на рис. 11-18), который эта роль предоставляет к защищаемым ей объектам. Например, если роль дает доступ на чтение к таблице через одну привилегию и полный доступ через другую, то эффективный уровень доступа к таблице – полный доступ. Таким образом, Просмотр результатов эффективного доступа показал бы эту таблицу с разрешениями на полный доступ. В табл. 11-4 приведены возможности, которые доступны из контекстного меню для различных объектов AOT. В левой колонке таблицы перечислены узлы AOT, а в остальных – доступные пункты меню.

Табл. 11–4. Пункты меню для артефактов контроля доступа

Название артефакта	**Просмотр связанных объектов безопасности**	**Просмотр связанных ролей безопасности**
Security\Role	Доступен	Не доступен
Security/Role\ <*НазваниеРои*>\Sub Roles	Доступен	Не доступен
Security\Duty	Доступен	Доступен

Табл. 11–4. Пункты меню для артефактов контроля доступа (*окончание*)

Название артефакта	Просмотр связанных объектов безопасности	Просмотр связанных ролей безопасности
Security\Privilege	Доступен	Доступен
Data Dictionary\Tables	Не доступен	Доступен
Forms	Не доступен	Доступен
Menu Items (Display, Output, Action)	Доступен	Доступен
Web\Web Menu Items (URLs, Actions)	Доступен	Доступен
Web\Web Content\Managed	Доступен	Доступен
Data Dictionary\Views	Не доступен	Доступен
Parts\Info Parts	Не доступен	Доступен
SSRS\Reports\<*Название-Отчета*>\Design	Не доступен	Доступен
Web\Web Files\Web controls	Не доступен	Доступен
Services\<*НазваниеСервиса*>\Operations\ <*ЛюбаяОперация*>	Доступен	Доступен

Отладка ролей безопасности

Отлаживать обычный код X++ вы можете в отладчике X++, если в Microsoft Dynamics AX вам назначена роль *Системный администратор*. Однако при работе в Microsoft Dynamics AX в качестве системного администратора вы не можете отлаживать инциденты, связанные с ролями безопасности, потому что запуск клиента Microsoft Dynamics AX под системным администратором никак не ограничивает доступ к функциональности. Чтобы решить эту проблему, выберите пользователя, которому назначена роль *Системный администратор*, назначьте ему дополнительную роль, которую вы хотите отладить (такую как *Бухгалтер*), и выполните следующие шаги.

1. Закройте все экземпляры клиента Microsoft Dynamics AX.
2. Запустите клиента Microsoft Dynamics AX и откройте рабочую область разработки.

3. Запустите еще один экземпляр клиента Microsoft Dynamics AX.
4. Добавьте вашему пользователю Microsoft Dynamics AX ту роль, которую хотите проверить.
   - Откройте Администрирование системы > Общие > Пользователи > Пользователи.
   - Дважды щелкните по коду вашего пользователя Microsoft Dynamics, чтобы открыть форму подробных сведений для вашей учетной записи.
   - Назначьте вашему пользователю Microsoft Dynamics AX ту роль, которую хотите проверить.
5. Закройте клиента Microsoft Dynamics AX.
6. В рабочей области разработки установите точки останова в коде X++, который вы хотите отладить.
7. Создайте и выполните job со следующей строкой кода:

```
SecurityUtil::sysAdminMode(false);
```

8. В рабочей области разработки нажмите Ctrl+W, чтобы открыть рабочую область приложения.

Теперь у вас открыт клиент с правами доступа той роли безопасности, которую вы хотите проверить, и при этом вы можете отлаживать код X++.

Примечание. Описанный подход работает для Windows-клиента Microsoft Dynamics AX, но не работает для Корпоративного портала или для кода, выполняемого через API-функцию *RunAs*.

Чтобы вернуть настройки к исходной роли *Системный администратор*, измените job, созданный на шаге 7, заменив значение параметра на *true*:

```
SecurityUtil::sysAdminMode(true);
```

С помощью указанной последовательности действий вы можете отлаживать приложение, запуская его в режиме, эмулирующем работу функционала для роли безопасности, которую вы хотите отладить.

Лицензирование и конфигурирование

В Microsoft Dynamics AX 2012 появилась новая модель лицензирования – лицензии для именованных пользователей. Эта модель предоставляет организации более простой способ лицензирования Microsoft Dynamics AX. В Microsoft Dynamics AX 2009 клиентам были доступны модели лицензирования по модулям, по числу одновременно работающих пользователей, а также так называемый business-ready (BRL). Для Microsoft Dynamics AX 2012 эти модели лицензирования более не применимы, вместо них были введены следующие модели.

- **Серверная лицензия.** Включает один экземпляр AOS. Дополнительные экземпляры AOS становятся доступны за счет приобретения дополнительных серверных лицензий.
- **Клиентская лицензия (Client Access License, CAL).** Дает именованному пользователю право доступа к определенному функционалу с любого числа устройств. Существуют четыре вида CAL (см. раздел «Типы клиентских лицензий» далее в этой главе). Просмотреть используемые в инсталляции клиентские лицензии вы можете с помощью отчета Администрирование системы > Отчеты > Лицензирование > Подсчеты лицензии пользователей с именем.
- **Лицензия на устройство (Device CAL).** Покрывает один экземпляр устройства.

Примечание. Назначение этого раздела – дать вам ясное общее представление о концепциях лицензионных ключей, конфигурационных ключей и типов клиентских лицензий с точки зрения разработчика. Более подробную информацию о ценах и требованиях к лицензированию вы можете найти в документе «Microsoft Dynamics AX 2012 Licensing Guide» по адресу: *http://www.microsoft.com/en-us/download/details.aspx?id=29859*.

Хотя лицензирование отдельных модулей более не используется, приложение все еще защищено лицензионными кодами (иногда называемыми *лицензионными ключами* или *кодами активации*). Лицензионные коды используются для активации Microsoft Dynamics AX 2012 в целом и отдельных наборов функций, доступных в продукте. Лицензионные коды отличаются от лицензированных прав пользования (то, что вы вправе ис-

пользовать, зависит от именованных пользовательских лицензий, которые вы приобрели). Когда вы получаете от Microsoft или компании-партнера файл с лицензионными кодами для активации программного обеспечения, то по умолчанию предоставляются лицензионные ключи на все наборы функций. Однако число пользователей, которым разрешено использовать продукт, и тип доступа, на который эти пользователи имеют право, зависит от именованных пользовательских лицензий. Снятие блокировки с лицензионного кода является первым шагом в настройке Microsoft Dynamics AX, потому что этот лицензионный код связан с конфигурационным ключом, который разблокирует набор функций. Ввести лицензионные коды вы можете с помощью формы лицензионных условий (рис. 11-19), доступной через меню Администрирование системы > Настройка > Лицензирование > Лицензионные условия.

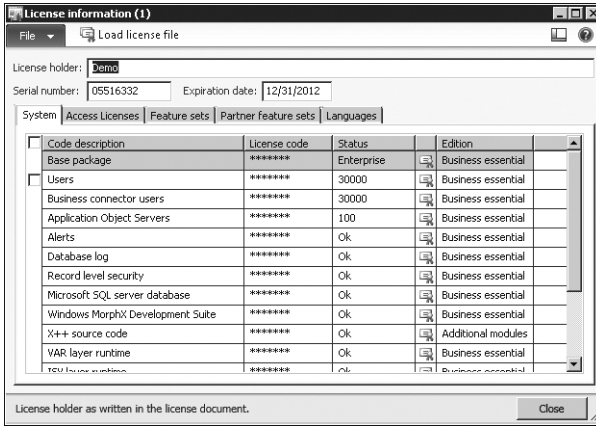

Рис. 11–19. Форма Лицензионные условия

Лицензионные коды вводятся вручную или импортируются из файла с помощью кнопки Загрузка файла лицензии. Все лицензионные коды и файлы лицензий, которые доступны для той или иной версии, генерируются в Microsoft. Лицензионные коды проверяются по отдельности с использованием информации о держателе лицензии, серийном номере, дате истечения срока действия лицензии и собственно лицензионном коде. В результате проверки либо лицензионный код принимается (и в поле статуса появляется значение счетчика, название или просто OK), либо в Infolog отображается сообщение об ошибке.

Примечание. Стандартные клиентские лицензии не содержат даты истечения срока действия. Такую дату содержат лицензии, предназначенные для иных целей, например ознакомительные, образовательные, для проектов независимых разработчиков ПО (ISV) и для проведения тренингов. При наступлении даты истечения срока действия лицензии режим работы системы изменяется, и она становится демонстрационным продуктом с ограниченной функциональностью.

Лицензионные коды делятся на пять групп (Система, Лицензии доступа, Наборы функций, Наборы функций партнеров и Языки) по типу функциональности, которую они представляют, как показано на рис. 11-19. Лицензионные коды создаются в AOT, и группировка определяется свойством лицензионного кода. Вкладка Наборы функций партнеров позволяет партнерам включать лицензированные партнерские модули. Инфраструктура лицензирования также может отслеживать зависимости между различными лицензионными кодами. У лицензионного кода может быть до пяти зависимостей от других лицензионных кодов. Добавление таких зависимостей позволяет избежать ситуаций, когда пользователи удаляют лицензионные коды и отключают наборы функций, от которых зависит другой набор функций.

Конфигурационная иерархия

Лицензионные коды находятся на вершине конфигурационной иерархии, являющейся отправной точкой для работы с системой конфигурирования, окружающей все модули приложения и системные компоненты, доступные в Microsoft Dynamics AX. Система конфигурирования базируется на примерно 300-х конфигурационных ключах, которые включают или отключают функциональность приложения в целом для всей инсталляции. Каждый конфигурационный ключ управляет доступом к определенному набору функций; при отключении конфигурационного ключа связанная с ним функциональность удаляется из пользовательского интерфейса (заметьте, что схема данных при этом не меняется, в отличие от Microsoft Dynamics AX 2009). Подсистема времени выполнения Microsoft Dynamics AX отображает элементы презентационной логики только для тех объектов приложения, которые связаны с включенным конфигурационным ключом либо не связаны ни с каким конфигурационным ключом.

Между лицензионными кодами, конфигурационными ключами и наборами функций – иерархическая связь. Отдельный лицензионный код не только позволяет включить множество конфигурационных ключей, но также и скрывает конфигурационные ключи и их функции по всей системе, если соответствующее значение лицензионного кода отсутствует или введено неверно. Сокрытие конфигурационных ключей с отсутствующими лицензионными кодами снижает сложность настройки. Например, если на форме Лицензионных условий лицензионный код введен неверно или не введен вовсе, то на форме Конфигурация не показываются конфигурационные ключи, связанные с этим кодом, а отображаются лишь корректные лицензионные коды и зависящие от них конфигурационные ключи. На рис. 11-20 показана типичная для проектов внедрений системы конфигурационная иерархия.

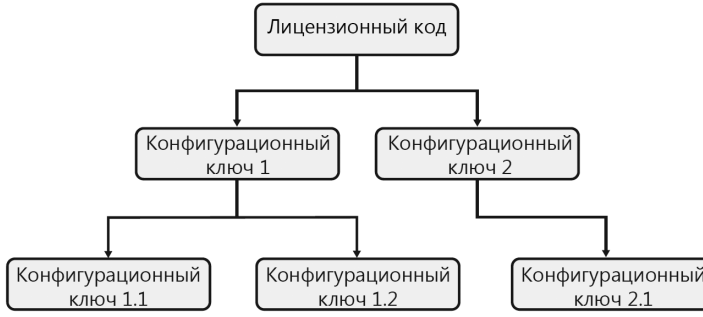

Рис. 11–20. Конфигурационная иерархия

Конфигурационные ключи

Модули приложения и связанная с ними бизнес-логика, включаемые с помощью лицензионных кодов и конфигурационных ключей, становятся доступны при развертывании Microsoft Dynamics AX. По умолчанию включены все лицензионные коды, но при этом включен лишь минимальный набор конфигурационных ключей. Если необходимо, то системный администратор должен включить дополнительные конфигурационные ключи во время установки и настройки системы. Внутри системы все, начиная от форм, отчетов и меню и заканчивая словарем данных, присутствует всегда, существуя во временном состоянии, пока соответствующие наборы функций не будут включены.

Когда вы включаете конфигурационный ключ, становится доступным набор функций, связанный с ним. Это означает, что при включении конфигурационного ключа становятся доступны соответствующие пункты меню, подменю, таблицы, кнопки и поля. Пользователю доступны лишь те области системы, к которым ему предоставлен доступ системным администратором через роли безопасности и которые включены с помощью конфигурационных ключей. Родительские конфигурационные ключи, показанные на рис. 11-20, связаны с лицензионными кодами. Удаление соответствующего лицензионного кода приводит к отключению связанных с ним родительских и дочерних конфигурационных ключей. Если лицензионный код не удален, то системный администратор может включать или отключать дочерние конфигурационные ключи, включая или отключая таким образом наборы функций, которые они представляют.

Примечание. Родительские конфигурационные ключи могут существовать без привязки к какому-либо лицензионному коду. Системный администратор может в любое время включать и отключать такие конфигурационные ключи на форме Конфигурация (рис. 11-21). Однако родительские конфигурационные ключи, связанные с лицензионным кодом, могут быть отключены только из формы Лицензионные условия.

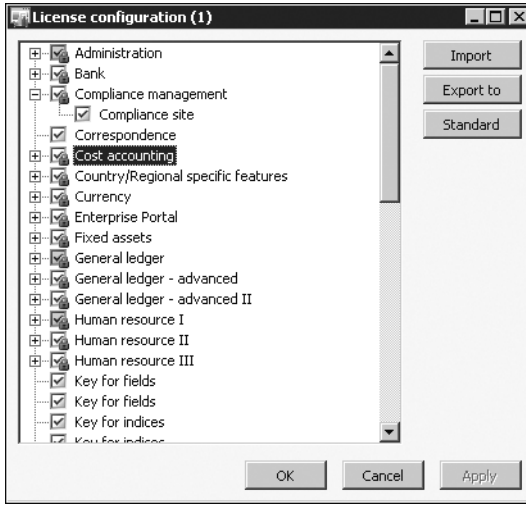

Рис. 11–21. Форма Конфигурация

В качестве более жизненного примера, представьте себе компанию, которой нужна большая часть функций модуля Торговля, но которая не торгует с зарубежными странами или другими регионами. Соответственно, компания решает не включать конфигурационный ключ Внешняя Торговля, который является дочерним ключом конфигурационного ключа Торговля. С использованием блок-схемы конфигурационных ключей из рис. 11.22 системный администратор может определить, будет ли конфигурационный ключ включен, и если нет, то во что обойдется его включение (что, в свою очередь, зависит от родительского конфигурационного ключа).

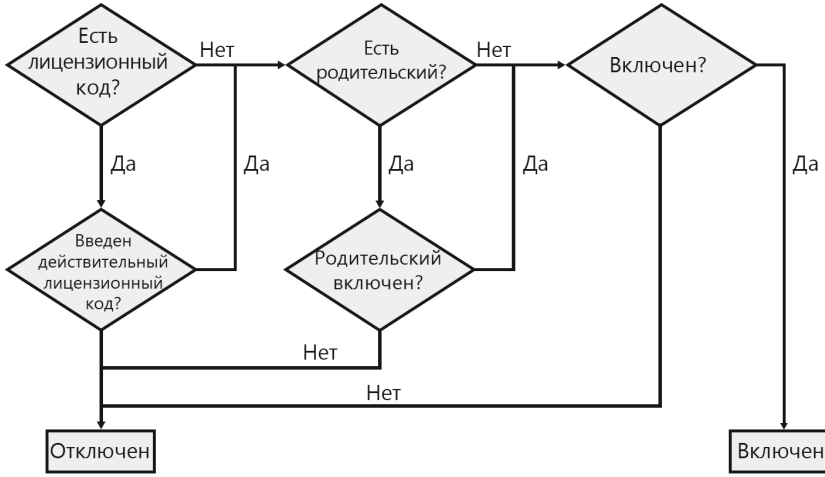

Рис. 11–22. Диаграмма проверки конфигурационных ключей

Использование конфигурационных ключей

Важной частью процесса разработки приложения является привязка расширений к конфигурационным ключам, которые интегрируют расширения в общее решение. Корректное использование конфигурационных ключей во всей системе может сделать широкомасштабные внедрения системы в корпорациях гибкими и менее затратными, при этом во всех подразделениях и регионах, на всех площадках смогут использовать одно и то же приложение, изменяя его под местные нужды с помощью конфигурационных ключей, а не разрабатывая модификации под каждую отдельную инсталляцию системы. Впрочем, полностью избежать локальных

доработок не удастся из-за особенностей бизнеса каждого подразделения или филиала и их специфических потребностей в доработках.

Конфигурационные ключи напрямую влияют на словарь данных, интерфейс и инфраструктуру навигации по приложению – вы можете привязать к конфигурационному ключу любой подходящий элемент приложения. В табл. 11-5 перечислены элементы, которые могут быть непосредственно привязаны к конфигурационному ключу.

Табл. 11–5. Ссылки на конфигурационные ключи

Группа типов элементов	Типы элементов
Словарь данных	Таблицы, включая поля и индексы Карты соответствия Отображения Расширенные типы данных Перечисления Конфигурационные ключи
Интерфейс и навигация в Windows-клиенте	Меню Пункты меню отображения Пункты меню вывода Пункты меню действия
Интерфейс и навигация в Web-клиенте	URL: Web menu items Action: Web menu items Display: Web content Output: Web content Web menus Weblets
Прочее	Одобрения документооборота Задачи документооборота Автоматизированные задачи документооборота Типы документооборота Ресурсы

Типы клиентских лицензий

Новая модель лицензирования на базе именованных пользовательских лицензий предоставляет клиентам возможность использовать все наборы функций приложения, при этом увязывая стоимость лицензий с числом пользователей, которые используют ту или иную функциональность, вместо того чтобы учитывать, включен ли в принципе определенный модуль. В этой модели лицензирования существуют четыре уровня клиентских

лицензий (CAL). Клиенты должны соблюдать условия лицензирования Microsoft за счет предоставления соответствующих прав доступа каждому пользователю. Доступны следующие уровни (типа пользователей), перечисленные в порядке убывания уровня доступа.

- **Enterprise (корпоративный).** Управляет бизнесом и отдельными процессами по всей организации.
- **Functional (функциональный).** Управляет бизнес-процессом внутри подразделения или бизнес-единицы.
- **Task (уровень задач).** Выполняет задачи по поддержке бизнес-процесса.
- **Self-serve (самообслуживание).** Управляет собственными персональными данными в рамках системы.

Все роли безопасности, идущие в стандартной поставке Microsoft Dynamics AX 2012, относятся к одному из этих четырех типов пользователей, давая, таким образом, вам возможность гибко лицензировать ваших пользователей в зависимости от того, как наиболее вероятно они будут использовать систему и извлекать из этого пользу.

Отображение пользовательской лицензии (CAL или же типа пользователя) на роль безопасности выполняется за счет того, что, во-первых, в свойствах пункта меню *ViewUserLicense* и *MaintainUserLicense* выбирается соответствующий тип пользователя. Во-вторых, по всей иерархии контроля доступа вычисляется наивысший уровень типа пользователя, который и становится для роли тем типом пользователя, на основании которого определяется необходимая пользовательская лицензия, как показано на рис. 11-23.

Как показано на рис. 11-23, Microsoft Dynamics AX 2012 отображает наборы пунктов меню на предопределенные роли, используя иерархию контроля доступа. В свойствах этих пунктов меню также указано одно из четырех значений, соответствующих типам пользователей. Каждое такое значение типа пользователя дает право выполнять действия, которые может делать только этот тип пользователя. Результирующий тип, требуемый для того или иного пользователя, определяется по наиболее высокому уровню из всех типов, которые встречаются в доступных этому пользователю пунктах меню. Например, чтобы добавлять новых рабочих (доступ к пункту меню *HcmWorkerNewWorker*), требуется уровень пользовательской лицензии Functional. Таким образом, эффективный тип пользователя для привилегии *HCMWorkerEdit* будет Functional, даже если она содержит

пункт меню *HcmWorker*, имеющий тип пользователя Task. Аналогично наивысший встречающийся тип пользователя проходит по всей иерархии контроля доступа и в конечном итоге становится эффективным типом пользователя для роли. В данном примере тип пользователя Functional является наивысшим в рамках роли *Помощник по управлению персоналом*, так что пользователю, которому назначается эта роль, требуется тип пользовательской лицензии Functional. У этого пользователя также будут лицензионные права на выполнение действий, которые относятся к более низким типам пользователей (таким как Task или Self-serve).

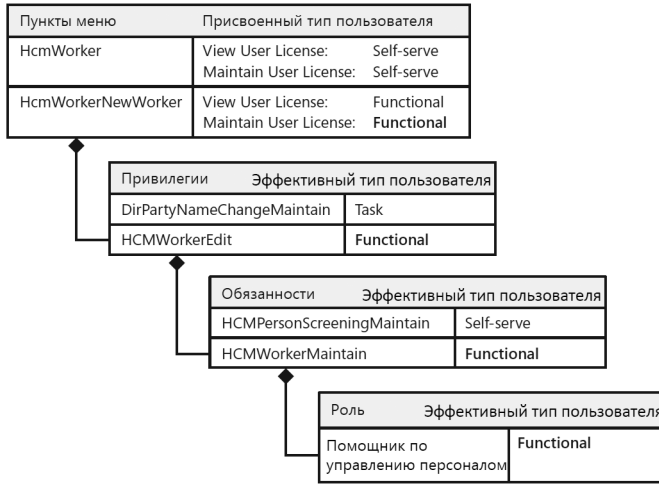

Рис. 11–23. Иерархия контроля доступа и типы пользователей

Кастомизации и лицензирование

С учетом того, что Microsoft Dynamics AX 2012 использует иерархию контроля доступа, а требования по лицензированию определяются пунктами меню, существует несколько ситуаций, при которых кастомизации могут повлиять на эти требования.

Изменение пунктов меню, связанных с ролью

В свойствах каждого пункта меню, включенного в Microsoft Dynamics AX 2012, указан соответствующий тип пользователя. Возможность изменения этих свойств на вышележащих слоях разработки намеренно отключена, однако вы можете изменять сами привилегии и роли, где встречаются

пункты меню. Когда пункт меню, идущий в стандартной поставке, перемещается в другую роль, то этой роли может потребоваться более высокий тип пользователя. Например, если пункт меню, помеченный типом пользователя **Enterprise, перемещается в роль, для которой прежде было достаточно** уровня пользователя Functional, то впоследствии эта роль тоже потребует уровня пользователя **Enterprise. Если же пункт меню перемещается** в роль, для которой изначально требуется равный или более высокий уровень пользователя, то никаких изменений в эффективном уровне пользователя, требуемом для роли, не происходит.

Примечание. Обычно только Microsoft использует именованные пользовательские лицензии в Microsoft Dynamics AX 2012 с целью определения необходимых условий лицензирования для клиента. В этом разделе приводятся сведения для разработчиков о том потенциальном воздействии, которое кастомизации могут оказать на лицензирование. Клиентам и партнерам не рекомендуется изменять соответствующие значения.

Изменение артефактов контроля доступа, связанных с ролью

Аналогично, если привилегии, обязанности или роли, содержащие пункты меню с различными типами пользователей, перемещаются из одной роли безопасности в другую, это может затронуть эффективный тип пользователя для роли. Если привилегия, прежде содержавшая пункты меню с уровнями типов пользователей вплоть до Functional, перемещается в роль с типом пользователя **Task, то для такой измененной роли теперь потребуется** пользовательская лицензия типа Functional.

Примечание. При добавлении новых пунктов меню на слое разработки для ISV или выше система позволяет вам изменять свойства *ViewUserLicense* и *MaintainUserLicense* этого пункта меню. Имейте в виду, что неправильное указание типов лицензий в ваших пунктах меню может отразиться на требованиях к лицензированию для компаний-клиентов. Клиентам и партнерам рекомендуется не указывать какие-либо значения типов лицензий в упомянутых выше свойствах. Кроме того, если пункт меню был создан на нижележащем слое разработки, то на текущем слое возможность задать в его свойствах более низкий тип пользователя также намеренно отключена.