СОВРЕМЕННЫЕ ТЕХНОЛОГИИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

УДК 004.438

РЕГЛАМЕНТАЦИЯ ДОСТУПА К ГРАФИЧЕСКИМ ОБЪЕКТАМ В ГЕОИНФОРМАЦИОННОЙ СИСТЕМЕ WINMAP

Д. А. Заставной

Южный Федеральный университет,
Ростовский филиал Российской Таможенной Академии

Поступила в редакцию 14.11.2016 г.

Аннотация. В статье рассмотрены разработанные методы регламентации доступа для геоинформационных систем. Описаны объектная модель целевой ГИС WinMAP и ее характерные особенности. В основу метода положена расширенная модель дискреционного доступа, адаптированная под архитектуру целевой ГИС. Так же приведены основные сведения о методах реализации и применения разработанных правил регламентации.
Ключевые слова: геоинформационные системы, информационная безопасность, дискреционная модель, регламентация доступа.
Annotation. This article describes the means of access control for a WinMAP geo-information system. The data object model of the system and its key features concerning the data security are described. The data access control model is an extended Discretion Access Control one adopted for the data model of the targeted GIS. An implementation of the extended DAC model is briefly sketched.
Keywords: geo-information system, data security, Discretion Access Control.

ВВЕДЕНИЕ

Одним из основных средств обеспечения безопасности в информационных системах является регламентация доступа к объектам (ресурсам) данной информационной системы; механизмы регламентации традиционно хорошо разработаны и эффективно используются в операционных системах и системах баз данных. Однако в геоинформационных системах [2, 6] и приложениях на их основе подобные средства не получили значительного распространения, что не соответствует ожидаемым требованиям на обеспечение, в частности, конфиденциальности в области применения этих систем. Кроме того, ГИС-системы и пространственные базы данных обладают некоторым специфическими особенностями, не имеющими аналогий в указанных выше системах, что предполагает создание и применение адекватных механизмов и технологий для регламентации доступа.

Традиционным средством регламентации доступа является модель дискреционного управления (Discretionary Access Control – DAC) [4], которое предполагает выделение набора объектов доступа (ресурсов) в информационной системе и определения троек

$$\langle o, s, m \rangle,$$

где s – субъект доступа, который можно ассоциировать с учетной записью и ее процессами, o – объект доступа (например, файл или таблица БД), и m – вид доступа (например, чтение или запись). Этот набор троек, собственно, и регламентирует правила доступа.

Данная модель чрезвычайно эффективно работает для атомарных, несвязанных между собой единиц данных, таких как файлы ОС

или объекты БД. Но для геоданных характерны такие взаимосвязи, например, как «объект А содержит в себе объект В»; так что если объект А является конфиденциальным, то и объект В может автоматически наследовать это свойство. Подобные зависимости, конечно же, могут быть выражены как расширение базовой модели DAC [3, 5] при помощи введения достаточно сложных регламентирующих правил, но их практическая реализация является весьма затратной с вычислительной точки зрения, поскольку подразумевает проверку взаимного пересечения большого количества геообъектов.

Вторая особенность связана с архитектурой практических приложений ГИС-систем; такие системы (напр. ArcGIS) для хранения данных используют репозиторий, надстраиваемый над традиционными SQL БД и другими источниками данных, что исторически привело к несколько нечетким и сложным способам регламентации доступа.

В данной статье представляются результаты по разработке системы регламентации доступа в геоинформационной системе WinMAP [1] с учетом архитектурных и функциональных особенностей данной системы. В основу регламентации положена модель DAC [4], расширенная правилами для поддержки геоассоциативных отношений, поддерживаемых данной ГИС. Целью этой разработки является создание простого и эффективного способа регламентации, который, помимо использования в целевой ГИС, мог бы бы перенесен и на другие системы аналогичной архитектуры.

Текст работы имеет следующую структуру. В Разделе 1 описана объектная модель ГИС WinMAP, ее архитектура и функциональные особенности. Раздел 2 посвящен детальному описанию способов регламентации доступа к системным привилегиям, объектам WinMAP и геоданным. Базовые сведения о прототипной реализации разработанных механизмов приведены в Разделе 3.

ОБЪЕКТНАЯ МОДЕЛЬ GIS WINMAP

Геоинформационная система WinMAP предназначена для управления данными и ресурсами, имеющими картографическую структуру, в таких традиционных сферах, как ведение земельного кадастра и управление ресурсами недвижимости, коммунальное хозяйство, и т. д. К ее основным функциональным возможностям относятся:

1. ввод, редактирование и визуализация геоданных, а так же растрового картографического изображения;

2. ввод и редактирование атрибутивных (семантических) данных, хранимых в виде таблиц;

3. выполнение поисковых операций по принципам «от картографического изображения к таблицам» и «от таблиц к картографическому изображению»;

4. создание экранных форм для доступа к атрибутивной информации;

5. формирование отчетов.

Система WinMAP в качестве репозитория может использовать системы баз данных Oracle, MS SQLServer и Access, а так же БД внутреннего формата. Следует отметить, что система безопасности WinMAP не использует соответствующие средства указанных систем.

На рис. 1. приведен пример, иллюстрирующий использование системы WinMAP в сфере управления городскими газовыми коммуникациями.

Графическими объектами, или геообъектами, называются визуализируемые в виде растрового изображения геометрические примитивы традиционных категорий – точки, визуализируемые в виде растровых иконок, мульти-полилинии (набор линий, или контуров, не являющихся в топологическом смысле связанными), и мульти-полигоны (набор полигонов, – замкнутых контуров). Графические объекты определяются набором точек в прямоугольной системе координат. Графический объект так же имеет несколько семантических атрибутов фиксированного набора (название, номер, надпись, и др.).

Особенностью объектной модели WinMAP является типизация графических объектов;

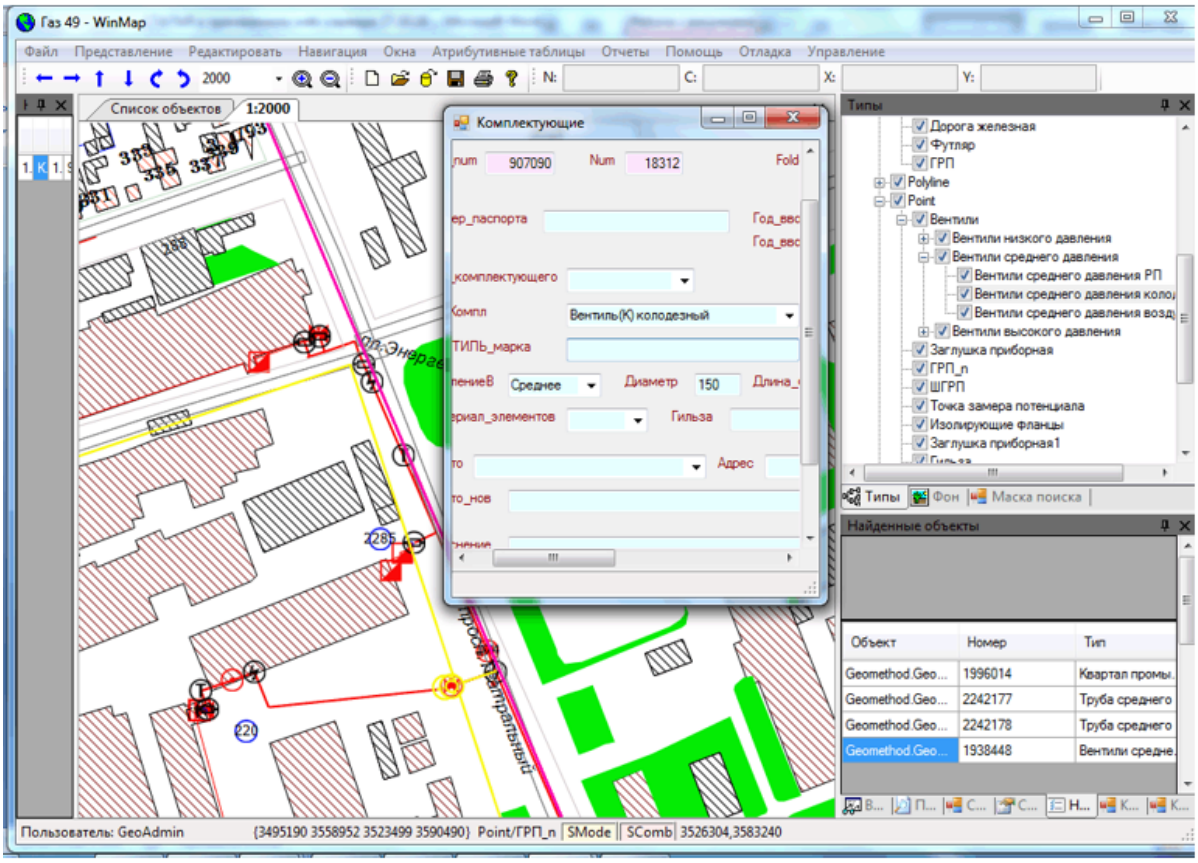

Рис. 1. Пример использования ГИС WinMAP

это означает, что графический объект создается как экземпляр типа, определяющего его семантику, а так же правила визуализации. Примерами типов являются «Постройки жилые», «Трубы надземные низкого давления», «Геодезические знаки».

Графические объекты образуют списки, получившие исторические название «кадастры». Распределение объектов по кадастрам не связано с их типами; кадастр можно считать логической частью общей базы данных графических объектов. Использование кадастров позволяет разделять графические объекты на логически связанные стабильные множества.

К дополнению к фиксированным атрибутам графических объектов используются расширенные атрибуты, хранимые в виде записей в соответствующих атрибутивных таблицах. Например, объект типа «Трубы надземные низкого давления» может иметь соответствующую запись в таблице «Трубы», содержащую специфическую для такого объекта информацию.

Графические объекты могут образовывать группы – набор объектов произвольных типов. Например, объекты, соответствующие некоторой газовой трубе, – собственно труба, многочисленные отводы от нее, задвижки, и прочие весьма многочисленные составляющие можно объединить в группу. Этой группой можно далее манипулировать как одним объектов, например, сдвигать. Отметим, что операция группировки широко используется в трехмерном моделировании, но в ГИС-системах получила незаслуженно малое внимание.

Еще одним специфическим объектом WinMAP является покрытие, – некоторый мульти-полигон, который определяет часть поверхности карты. Например, графический объект типа «Промышленный квартал» может быть объявлен как покрытие.

Группы и покрытия являются сходными объектами с точки зрения возможности манипулирования входящими в них объектами; отличия состоят в определении принадлежности объектов к группе или покрытию.

В группу объект включается явно, и проверка вхождения объекта в группу проверяется тривиальным способом. Вхождение же объекта в покрытие определяется неявно, через проверку пересечения или вхождения этого объекта в границу покрытия при помощи координат. Группы и покрытия могут содержать только графические объекты, но не другие группы и покрытия. Объект может входить только в одну группу или покрытие.

Следует иметь в виду, что любой графический объект обязательно входит в коллекцию-тип, но его вхождение в какую-либо группу или покрытие на практике бывает достаточно редко.

Кадастры, типы, атрибутивные таблицы, группы и покрытия будем далее называть коллекциями.

РЕГЛАМЕНТАЦИЯ ДОСТУПА В СИСТЕМЕ WINMAP

К средствам обеспечения безопасности в системе WinMAP относятся:

1. Средства для авторизации и аутентификации и управления учетными записями.

2. Средства для регламентации доступа и собственно монитор проверки разрешений.

3. Средства аудита.

В данной статье основное внимание уделяется принципам и механизмам регламентации доступа и правила проверки разрешений доступа.

Объектами регламентации, согласно представляемой концепции, являются:

1. привилегии (политики);

2. коллекции (кадастры, типы, группы и покрытия, атрибутивные таблицы);

3. графические объекты;

4. атрибутивные записи.

Привилегиями называются действия по созданию, удалению, модификации и изменению статуса соответствующей коллекции и индивидуальных графических объектов и атрибутивных записей. Например, предоставление привилегии «создание типа» позволяет пользователю создавать новые типы. Данные действия (создание, удаление, модификация) не имеют отношения к регламентации доступа к графическим объектам и атрибутивным записям.

Доступ к графическим объектам может быть регламентирован на уровне коллекции, и на уровне индивидуального объекта. Для графических объектов определены следующие виды доступа:

1. просмотр объекта в виде изображения на электронной карте;

2. просмотр координат объекта;

3. просмотр собственных семантических атрибутов объекта;

4. редактирование координат объекта;

5. редактирование собственных семантических атрибутов объекта;

В отличие от традиционной модели DAC, объекты не имеют владельца, и, соответственно, нет привилегии типа «передача права владения». Однако действия по созданию объектов, записей и коллекций может быть подвержены аудиту.

Право доступа предоставляется либо для конкретной учетной записи, либо может быть объявлено публичным. По умолчанию, если для некоторого субъекта некоторое право доступа на объект не представлено явно, и это право не объявлено публичным, доступ отсутствует.

Право доступа на индивидуальный объект может иметь три значения:

1. Право предоставлено.

2. Право предоставлено в доминирующей форме.

3. Право запрещено в доминирующей форме.

Доминирующие разрешения и запрещения необходимы для определения доступа объектов через членства в коллекциях. Доминирующие предоставление права возможно только на уровне индивидуальный объектов, но не на уровне коллекций.

Права доступа на коллекции включают пять прав, повторяющих права на индивидуальный объекты, и права «создать объект (в коллекции)» и «удалить объект (из коллекции)», а так же права на некоторые специфические действия (например, перенос объекта из одного кадастра в другой). Отметим, что удаление объекта из типа приводит к полно-

му удалению его из ГИС, тогда как удаление их группы или покрытия просто переводит объект в «автономное» состояние, и он более не наследует свойства группы или покрытия. Из кадастра объекты удалять, естественно, нельзя, можно только перемещать в другой кадастр.

Аналогичным образом связаны права на индивидуальные атрибутивные записи и атрибутивные таблицы.

Типичным примером использования типов для обеспечения конфиденциальности является следующая схема: пользователем низкой категории доступа предоставляется информация о городских постройках, дорогах, водяных объектах, но не предоставляется доступ к типам, соответствующим газовым коммуникациям. В качестве применения группы можно использовать следующую ситуацию: пользователю предоставляется право на просмотр всех объектов газовой инфраструктуры, относящихся к конкретному газопроводу, но не вообще ко всем объектам «газовых» типов. Наконец, покрытие можно использовать для «сокрытия» фрагментов территорий, на которых находятся какие-либо непубличные организации.

Естественно, права на визуальный просмотр, просмотр координат и атрибутивной информации, и редактирование различаются.

Для кадастров и таблиц существует так же дополнительная привилегия «просмотр», которая позволяет просматривать все записи и выполнять поисковые операции (накладывание фильтров). Если право «просмотр» на кадастр не предусмотрено, это означает, что объекты этого кадастра (при выполнении прочих ограничений) будут воспроизводится на экране (это действие традиционно называется рендерингом), и при наличии соответствующих прав можно будет выбирать на экране отдельные объекты и просматривать их характеристики (собственные атрибуты и координаты), однако просматривать список всех объектов и выполнять поиск в этом списке будет нельзя. Аналогично, отсутствие права просмотра атрибутивной таблицы позволяет для индивидуальных графических объектов просматривать соответствующую запись с расширенной атрибутивной информацией, но запрещает просматривать все записи таблицы (и, соответственно, переходить к связанным графическим объектам).

Если для коллекции предоставлен право на некий вид доступа, каждый объект, в него входящий, наследует это право, если только для объекта не задано доминирующее запрещение этого права. Если для коллекции право на вид доступа не предоставлено, объект получает это право, если ему было предоставлено доминирующее разрешение на этот вид доступа.

Теперь опишем (неформально) правила рендеринга графических объектов, как на наиболее характерную для ГИС-систем операцию и как наиболее трудоемкую. Объект прорисовывается (для данного субъекта доступа), если:

1. Он предоставлен в публичный доступ.
2. Он имеет доминирующее разрешение.
3. Он входит в коллекцию, для которой разрешен рендеринг, и объект не имеет доминирующего запрещения для прорисовки.

Прокомментируем приведенные правила. Действительно, очень многие графические объекты могут быть предоставлены в публичный доступ, как не являющиеся конфиденциальными, по крайней мере для авторизированных пользователей ГИС; сами по себе карты (в отличие от координат и атрибутивных данных) обычно не являются секретными. Объекты, для которых предоставлено доминирующее разрешение, будут прорисовываться вне зависимости от прав, предоставленных содержащих его коллекциям. Однако без этого разрешения они не будут прорисовываться, если входят в непрорисовываемую коллекцию.

РЕАЛИЗАЦИЯ ХРАНЕНИЯ ПРАВ И ПРОВЕРКИ

Реализация системы регламентации доступа включает два важных аспекта, кратко описываемых в этом разделе, - представление и хранение прав доступа на объекты, и механизм проверки вхождения графических объектов и атрибутивных записей в коллекции.

Права доступа представляются, как и права доступа на файлы в операционных системах, в виде списков доступа (Access Control List, ACL), которые хранятся вместе с объектами. В репозитории WinMAP права доступа хранятся в отдельных структурах данных, но после загрузки объектов в оперативную память списки доступа графических объектов хранятся вместе с ними; списки доступа на записи таблиц хранятся отдельно. Список доступа графического объекта содержит:

1. признак публичности.
2. идентификатор типа.
3. идентификатор кадастра
4. идентификатор группы или покрытия, если он в них входит.
5. собственные права, представленные в виде списка пар (идентификатор субъекта, идентификатор вида доступа).

Списки доступа коллекций представлены аналогичным способом.

Проверка вхождения объекта в коллекцию реализованы следующим образом. Идентификаторы кадастра и типа всегда присутствуют в объекте, как идентификаторы группы или покрытия. Группа, в свою очередь, реализована как список идентификаторов объектов, перебор которых производится очень быстро. Покрытия устроены несколько сложнее; они определяются границей мульти-полигоном, в которую входят другие графические объекты.

Проверка вхождения является достаточно сложными при выполнении двух условий:

1. Проверка выполняется в пространственной базе данных, а не в оперативной памяти.
2. Проверка выполняется транзитивно.

В системе WinMAP транзитивных вложенностей нет, что сделано специально для упрощения этой проверки; автор полагает, что на практике достаточно иметь один объект-границу, объявленную конфиденциальной. Кроме того, учитывая достаточную стабильность данных (отсутствие частых изменений большого количества данных об объектах), объекты-покрытия очень эффективно индексируются. В системе WinMAP покрытие реализовано так же, как и группа (в виде списка идентификаторов), но вхождение других объектов в нее осуществляется один раз при ее создании, с последующей корректировкой при добавлении новых графических объектов. Наконец, по опыту автора, объем пространственных баз данных, используемых во многих современных приложениях, вполне допускает загрузку всех графических объектов целиком в оперативную память.

ЗАКЛЮЧЕНИЕ

В работе представлены результаты разработки системы регламентации доступа к данным пространственной базы данных, разработанной для ГИС WinMAP. Использование специфических структур данных этой системы позволяет реализовать эффективные и удобные методы реализации. Некоторые вопросы, представляющие потенциальный интерес, например, разработка модели разграничения на основе меток безопасности, остались за рамками исследования, но при необходимости разработанная модели может быть расширена для реализации указанных средств.

СПИСОК ЛИТЕРАТУРЫ

1. *Заставной Д. А.* Встроенный язык скриптов для GIS-системы WinMap./ Д.А.Заставной. // Известия ЮФУ. Технические науки. – 2011. – № 1. – С. 144–150.

2. *Шаши Шекхар, Санжей Чаула.* Основы пространственных баз данных / Шаши Шекхар, Санжей Чаула. – М. : Кудриц-Образ, 2004. – 428 с.

3. *Deren Li; Jianya Gong; Huayi Wu.* View-based access control mechanism for spatial database/ Deren Li; Jianya Gong; Huayi Wu. – Режим доступа: http://www.isprs.org/proceedings/XXXVII/congress/8_pdf/5_WG-VIII-5/02.pdf.

4. *Ravi S. Sandhu, Pierangela Samarati.* Access Control: Principles and Practice/ Ravi S. Sandhu, Pierangela Samarati // IEEE Comunication Magazine. – 1994. – P. 40–48.

5. *Liliana Kasumi Sasaoka, Claudia Bauzer Medeiros.* Access Control in Geographic Databases / Liliana Kasumi Sasaoka, Claudia Bauzer Medeiros// Advances in Conceptual Modeling – Theory and Practice. Lecture Notes in Computer Science. Springer. – 2006. – Vol. 4231. – P. 110–119.

6. *ДеМерс Майкл Н.* Географические информационные системы. Основы / ДеМерс Майкл Н. Пер. с англ. – М. : Дата+, 1999. – 478 с.

Заставной Д. А. – канд. техн. наук, доцент кафедры информатики и вычислительного эксперимента Института математики, механики и компьютерных наук им. И. И. Воровича Южного Федерального университета; Ростовский филиал Российской Таможенной Академии.
E-main: dzast@sfedu.ru

Zastavnoy D. A. – PhD in Computer Science, Associate Professor of Informatics and Computer Experiment Department, Institute for Mathematics, Mechanics, and Computer Science in the name of I.I. Vorovich, South Federal University; Russian Academy of Custom Service.
E-main: dzast@sfedu.ru