DOI: 10.12737/22826

Заставной Д.А., канд. техн. наук, доц.
Южный федеральный университет

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГЕОИНФОРМАЦИОННОЙ СИСТЕМЕ WINMAP

dzast@sfedu.ru

Одной из важнейших задач современных информационных систем является обеспечение информационной безопасности. В области геоинформационных систем и пространственных баз данных и их практических приложений, однако, методы обеспечения безопасности получили недостаточное развитие. В значительной степени это обусловлено особенностями моделей конфиденциальности для геометрически связанных пространственных объектов. В данной статье предлагается последовательное описание средств обеспечения безопасности для системы ГИС WinMAP, к которым относятся идентификация и аутентификация пользователей, регламентация доступа субъектов к ресурсам системы, и аудит. В основу модели безопасности положена модель дискреционного управления доступом (DAC). Статья включает краткое описания объектной модели указанной ГИС и специфических структур данных, введение которых позволяют существенно упростить методы регламентации, а так же реализацию их проверок в реальной системе. Для иллюстрации методов управления доступом используются команды скриптового языка системы.

Ключевые слова: *GIS-системы, пространственные базы данных, информационная безопасность, дискреционная модель управления доступом.*

Введение.

В настоящее время значительное распространение получили практические приложения на основе геоинформационых систем в различных областях, включая такие сферы, как управление земельными и природными ресурсами, объектами недвижимости, городской инфраструктурой. Данные ГИС-систем традиционно включают графические объекты, образующие электронные карты, и семантическую (атрибутивную) информацию [1,2]. Поскольку подобные данные весьма часто являются конфиденциальными, естественной необходимостью является разработка и использование методов обеспечения информационной безопасности, в особенности, если речь идет о профессиональных системах.

Методы обеспечения безопасности получили вполне завершенное и целостное развитие, например, в системах баз данных и в операционных системах. К основным средствам относится управления учетными записями, авторизация пользователей, регламентации доступа пользователей к объектам системы, аудита, а так же криптографические средства и аспекты сетевой безопасности (в данной работе не затрагиваемые). Наиболее важное и содержательное место среди них занимает задача регламентации доступа.

Теоретической основой регламентации доступа является так называемая модель дискреционного управления (Discretionary Access Control - DAC) [3]. Согласно этой модели, для каждого объекта доступа (файла ОС, таблицы БД) и для каждого субъекта (зарегистрированного пользователя) должно быть задан вид доступа (чтение, запись, и т.д.), который разрешен данному субъекту применительно к данному объекту. Отсутствие предоставленного права означает запрет доступа.

Данная модель очень удобна для практического использования и эффективно реализуется, если объекты доступа являются атомарными, и конфиденциальность одного объекта не влияет на конфиденциальность другого. Однако для ГИС-систем типичны следующие ограничения: объект является конфиденциальным, и, следовательно, все объекты, находящиеся внутри этого объекта, так же должны считаться конфиденциальными. Подобные правила вполне могут быть введены в модели безопасности, однако их практическое использование будет связано с необходимостью выполнения многочисленных проверок вхождения, что является вычислительно сложной задачей [4].

В данной статье описаны базовые средства обеспечения безопасности, включая расширенный метод DAC, адаптированный для специфических структур данных этой системы. Так же приводятся примеры использования этих средств, реализованных в виде расширения скриптового языка, введенного автором в статье [5].

Основная часть.

Важной особенностью подхода, принятого в статье, состоит не в разработке общих методов обеспечения конфиденциальности в сфере ГИС и пространственных баз данных, а в развитии и

адаптации хорошо зарекомендовавших себя принципов применительно к конкретной системе. Поэтому перед детальным рассмотрением разработанных средств следует описать основные архитектурные особенности модели данных WinMAP.

Атомарными структурами данных WinMAP являются графические объекты и атрибутивные записи. Графический объект определяется набором координат в прямоугольной системе, и набором собственных семантических атрибутов, который является фиксированным по структуре для всех объектов. Дополнительные атрибуты могут храниться в атрибутивных таблицах.

На основе графических объектов образуются коллекции, к которым относятся: кадастры, типы, группы и покрытия. Кадастр является логическим разделом базы данных объектов, что удобно как с точки зрения практического использования, так и с точки зрения ограничения доступа. Типичная структура БД системы WinMAP состоит из нескольких кадастров, среди которых может быть кадастр с архивными неизменяемыми данными, кадастр с оперативно используемыми объектами, и т.д.

Графический тип определяет семантическую категорию объектов, и задает правила визуализации (прорисовки) объектов; любой объект создается как экземпляр некоторого типа. Конкретный графический объект всегда принадлежит одному и только одному типу, равно как и только одному кадастру. Примером типов являются «Жилые постройки» и «Газовые трубы низкого давления».

Дополнительными видами коллекций, членство объектов в которых не является обязательным, являются группы и покрытия. Группа – это именованный набор объектов, которые включаются в группу явно. Объекты в группе наследуют геометрические трансформации группы (напр., перемещение), что очень удобно для манипулирования с ними. Например, в некую группу можно включить конкретную газовую трубу, все отводы, задвижки, и прочие относящиеся к ней многочисленные объекты газовой инфраструктуры.

Покрытия по своим свойствам напоминают группы, но объекты в них включаются неявно, – при помощи проверки геометрического вхождения объекта в границу покрытия, заданного другим графическим объектов. Типичным примером покрытия можно назвать объект – «Промышленный квартал», в который входит множество построек и прочих объектов. При вводе (или импорте) графического объекта внутрь объекта-покрытия он автоматически становится его членом. Такой способ позволяет избегать постоянных проверок взаимного вхождения объектов, что фундаментально упрощает как манипулирование с объектами покрытия, так и регламентацию доступа. Следует иметь в виду, что графические объекты по редко подвергаются модификации, так что их членство в покрытиях весьма стабильно.

Теперь перейдем к описанию собственно разработанных средств обеспечения безопасности, к которым относятся управление учетными записями, регламентация доступа и аудит.

Учетные записи содержат следующие сведения: имя учетной записи (логин), детальное описание владельца, внутренний идентификатор, пароль в виде криптографической хеш-функции, вычисляемой по алгоритму MD5, а так же дополнительные атрибуты. Создание и прочие манипуляции с учетной записью могут осуществляться при помощи оконных средств, или при помощи соответствующих команд интерпретатора. При входе пользователя в систему происходит авторизация, и дельнейшие действия пользователя, в частности, проверка прав доступа и регистрация событий аудита, происходит с использованием идентификатора учетной записи.

Специальным видом учетной записи является административная учетная запись, с помощью которой можно создавать и модифицировать другие учетные записи, а так же выполнять некоторые технические действия по обслуживанию системы (например, импорт и экспорт данных).

В основу регламентации доступа положена дискреционная модель [3,4], расширенная дополнительными средствами, учитывающими специфические особенности пространственных данных. Объектами регламентации, согласно представляемой концепции, являются:

1. привилегии (политики);
2. графические объекты;
3. атрибутивные записи;
4. коллекции (кадастры, типы, группы и покрытия, атрибутивные таблицы).

Привилегиями называются права на выполнение действий, не связанных с конкретными данными, в том числе создание, удаление и изменение коллекций, атрибутивных таблиц, графических объектов и записей.

Для графических объектов определены следующие виды доступа:

1. просмотр изображения на карте (прорисовка);
2. просмотр собственных атрибутов;
3. просмотр координат;
4. редактирование объекта;
5. редактирование собственных атрибутов.

Очевидно, что при такой схеме видом доступа достаточно удобно разграничивать возможность просмотра картографического изображения, которое само по себе редко является конфиденциальным, и возможность просмотра и редактирования координат и семантических атрибутов, которые часто бывают конфиденциальными.

Каждый вид доступа на графический объект может быть представлен одной из трех форм: доступ представлен, доступ представлен в доминирующей форме, и доступ запрещен в доминирующей форме.

Для коллекций и атрибутивных таблиц определены, в том числе, виды доступа «прорисовка», «включение (создание) объекта», «исключение (удаление) объекта», «модификация элемента», «просмотр коллекции»; последний вид доступа подразумевает просмотр элементов коллекции в виде списка и поиск при помощи накладывания фильтров.

Права доступа, предоставленные коллекции и входящим в него элементам, связаны следующим образом. 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.

Право на объект или привилегию может быть так же предоставлено для публичного доступа; в этом случае любой пользователь автоматически получает это право, если только оно не было запрещено для него в доминирующей форме. Это весьма удобно с практической точки зрения, поскольку на практике большинство географических данных не является конфиденциальными для авторизированных пользователей.

Поскольку наиболее типичным и характерным видом доступа является просмотр множества графических объектов в виде растрового изображения, образующего карту, рассмотрим неформально алгоритм определения прав прорисовки объектов с учетов их членства в коллекциях. Для заданного субъекта доступа графический объект прорисовывается, если:

1. Объект предоставлен в публичный доступ.
2. Объект имеет доминирующее разрешение.
3. Объект входит в коллекцию, для которой разрешена прорисовка, и объект не имеет доминирующего запрещения для этого вида доступа.

Описанная модель регламентации доступа допускает достаточно простую и эффективную реализацию. С каждым объектом доступа ассоциирован список доступа (ACL), содержащим идентификаторы учетных записей, маски доступа и форм их предоставления. При прорисовке происходит последовательный перебор объектов коллекций (поскольку прорисовка выполняется не на уровне одиночных объектов, а на уровне коллекций) и сопоставление прав графических объектов и прав коллекций согласно описанному выше алгоритму для формирования итогового права доступа. Поскольку вхождение объектов в покрытия, предназначенных для моделирования «конфиденциальных зон», определяется только один раз (при создании объекта и помещении его в покрытие), дальнейшие проверки являются тривиальной задачей.

В отличие от традиционной модели DAC, объекты доступа не имеют владельца. Однако действия по созданию, удалению и модификации графических объектов, записей и коллекций может быть подвержены аудиту. Аудит заключается в накапливании в специальной таблице сведений о следующих событиях:

1. Регистрация пользователя в системе и выход из нее (включая неудачные попытки).
2. Создание, удаление и модификация коллекций и атрибутивных таблиц.
3. Изменение сведений об учетных записях.
4. Импорт и экспорт данных.
5. Доступ к графическим объектам, атрибутивным записям и коллекциям (отдельно по всем видами доступа, перечисленным выше).

Аудит доступ к публичным объектам не выполняется.

По умолчанию аудит не включен, что обусловлено очевидными вычислительными затратами на журнализацию событий. Для активации аудита, которое выполняется администратором, необходимо выбрать соответствующий объект аудита в соответствующем списке и активировать необходимые опции – виды доступа, форма предоставления, учетные записи, результат попытки получать право доступа. После включения аудита соответствующие записи добавляются в журнал.

Функции управления безопасности доступны при помощи соответствующих оконных инструментов, а так же при помощи команд скриптового языка, описанного в работе [5]. Применение скриптовых языков существенно развивает функциональные возможности ГИС-систем, позволяя выполнять разнообразные манипулирования с данными. Отметим, что на выполнение команд скриптового языка так же распространяется правила регламентации доступа и

аудита, но подробное описание этих аспектов выходит за пределы данной статьи.

Ниже приведены примеры команд с комментариями.

```
-- создание учетной записи
GISUser Alise = new GISUser( “Alice”, “ToughPassword” );
-- предоставление созданной учетной записи привилегии создания типов и групп
Policy.GrantPermission( Alice, CREATE_GTYPE );
Policy.GrantPermission( Alice, CREATE_GROUP );
-- удаление права создания типов
Policy.RevokePermission( Alice, CREATE_GTYPE );
-- предоставление права создавать объекты указанного типа
Object.GrantPermission( Alice, GTYPE, “Трубы низкого давления”, ADD );
-- предоставление права прорисовки объектов этого типа
Object.GrantPermission( Alice, GTYPE, “Трубы низкого давления”, RENDER);
-- запрещение редактирования координат графического объекта (объект
-- идентифицируется при помощи номера)
Object.RevokePermission( Alice, GOBJECT, 514601, EDITPOINTS );
-- активация аудита редактирования этого объекта
Audit.Activate(Alice, GOBJECT, 514601, EDITPOINTS, ALL );
```

Выводы. В работе представлены результаты разработки средств для обеспечения информационной безопасности в геоинформационной системы WinMAP, включающие расширенную модель дискреционного доступа, адаптированную для ГИС-систем. Показана возможность эффективной реализации проверки прав доступа, что реализуется благодаря введению специфических структур данных. Разработанные средства могут практически использоваться, в том числе, при помощи команд скрипового языка системы WinMAP.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ДеМерс Майкл Н. Географические информационные системы. Основы. Пер. с англ. М., Дата+, 1999. 478 с.

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

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

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

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

Zastavnoy D.A.

DATA SECURITY SYSTEM FOR THE WINMAP GIS

A key feature for the information systems is data security, but the Geoinformation Systems and Spatial Databases as well as their applications appear to have some drawbacks concerning that matter. Most suggestions about geodata confidentiality are obviously stuck in their attempts to link access rules with geometric properties of spatial data. In this paper we suggest a different approach toward build data access model and a complete data security system for a WinMAP system which includes account control, data access control based on an extended DAC and audit features. A data model of WinMAP is also described because its specialized features allow to rationally develop and effectively implement the data security system. An implementation of the extended DAC model is briefly sketched.

***Key words**: Geo-information system, spatial databases, data security, Discretion Access Control.*

Заставной Дмитрий Александрович, кандидат технических наук, доцент кафедры информатики и вычислительного эксперимента института математики, механики и компьютерных наук им. И.И. Воровича.
Южный Федеральный Университет.
Адрес: Россия, 344090, Ростов-на-Дону, ул. Мильчакова, д. 8а.
E-mail: dzast@sfedu.ru