УДК 004.42

О.И. Жуковский, Ю.Б. Гриценко

Особенности создания системы информационной безопасности веб-ГИС ведения электронного генерального плана инженерной инфраструктуры

Представлена задача оценки применимости моделей доступа для системы информационной безопасности веб-ГИС ведения электронного генерального плана предприятия. Рассмотрены основные модели доступа, применяемые при проектировании и создании современных автоматизированных информационных систем, используемых на крупных промышлен-ных предприятиях. Представлены возможности системы информационной безопасности веб-ГИС системы ведения электронного генерального плана, разработанной на основе одной из рассматриваемых моделей доступа.

Ключевые слова: электронный генеральный план, геоинформационная система, модель доступа, ролевая модель.

Построение современных геоинформационных систем (ГИС) управления инженерной инфраструктурой предприятия тесно связано с проблемой обеспечения информационной безопасности. Разноплановость данных электронного генерального плана (ЭГП) как основной формы представления инженерной инфраструктуры, разнообразие решаемых с его помощью производственных задач, широкий круг потенциальных его пользователей заставляют особенно тщательно относиться к решению данной задачи [1]. Одним из основных моментов, определяющих ее успешное решение, является применение формальных моделей безопасности на всех этапах жизненного цикла системы, особенно на этапе проектирования. При этом наиболее важным является использование формальных моделей при проектировании систем контроля и управления доступом.

Формальные модели безопасности играют важную роль в процессах проектирования, разработки, сертификации и исследования защищенной ГИС, так как обеспечивают системотехнический подход, включающий решение такой задачи, как выбор и обоснование базовых принципов архитектуры защищенной ГИС, определяющих механизмы реализации средств и методов защиты информации от несанкционированного доступа.

Среди формальных моделей безопасности выделяют модели управления доступом. Модели этого класса предназначены для обеспечения решения задач анализа и синтеза систем (механизмов) разграничения доступа к различным видам ресурсов ГИС. Выделение этих моделей в самостоятельный класс общих моделей обусловлено тем, что механизмы разграничения доступа относятся к числу наиболее существенных компонентов систем защиты информации, от эффективности функционирования которых в значительной мере зависит общая эффективность защиты информации.

Постановка задачи. Несмотря на достаточно высокий уровень теоретических исследований в области формальных моделей доступа, их практическая реализация наталкивается на существенные трудности, связанные с особенностями как разрабатываемой системы, так и объекта информатизации. Рассмотрим применимость наиболее востребованных в настоящее время моделей доступа для проектирования и создания веб-ГИС ведения электронного генерального плана предприятия.

Основными формальными моделями управления доступом, используемыми в современных компьютерных системах, являются дискреционные, мандатные и ролевые модели [2–8]. Для рассмотрения данных моделей безопасности будем использовать принятые в настоящее время следующие базовые представления.

Система является совокупностью взаимодействующих сущностей субъектов и объектов. При таком представлении системы безопасность обработки информации обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с заданным набором правил и ограничений, которые образуют политику безопасности. Считается, что система безопасна, если субъекты не имеют возможности нарушить правила политики безопасности. Общим подходом для всех моделей является разделение множества сущностей, составляющих систему, на множества

субъектов и объектов, хотя сами определения понятий «объект» и «субъект» в разных моделях могут существенно различаться.

1. Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов отношений определяется в виде набора опера-ций, которые субъекты могут производить над объектами.

2. Все операции контролируются монитором взаимодействий и либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.

3. Политика безопасности задается в виде правил, в соответствии с которыми должны осуществляться все взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.

4. Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет состояние системы. Каждое состояние системы является либо безопасным, либо небезопасным в соответствии с предложенным в модели критерием безопасности.

5. Основной элемент модели безопасности – это доказательство утверждения о том, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

Опираясь на указанные базовые понятия, рассмотрим возможности применения основных моделей управления доступом для построения системы информационной безопасности веб-ГИС ведения электронного генерального плана инженерной инфраструктуры.

Рассмотрение моделей доступа

Дискреционные модели реализуют дискреционное управление доступом, основанное на заданном множестве отношений доступа. Классической дискреционной моделью является модель Харрисона–Руззо–Ульмана [4, 9], которая помимо произвольного управления доступом субъектов к объектам осуществляет контроль над распространением прав доступа. В рамках этой модели система обработки информации представляется в виде совокупности активных сущностей – субъектов (множество **S**), которые осуществляют доступ к информации, пассивных сущностей – объектов (множество **O**), содержащих защищаемую информацию, и конечного множества прав доступа **R**, означающих полномочия на выполнение соответствующих действий (например, чтение, запись, выполнение). Причем для того, чтобы включить в область действия модели и отношения между субъектами, принято считать, что все субъекты одновременно являются и объектами.

Поведение системы моделируется с помощью понятия «состояния». Пространство состояний системы образуется декартовым произведением множеств составляющих ее объектов, субъектов и прав. Текущее состояние системы **Q** в этом пространстве определяется тройкой, состоящей из множества субъектов, множества объектов и матрицы прав доступа **M**, описывающей текущие права доступа субъектов к объектам, – **Q** = (**S**, **O**, **M**). Строки матрицы соответствуют субъектам, а столбцы – объектам, поскольку множество объектов включает в себя множество субъектов, матрица имеет вид прямоугольника. Любая ячейка матрицы **M**[*s*, *o*] содержит набор прав субъекта **S** к объекту **O**, принадлежащих множеству прав доступа **R**.

Поведение системы во времени моделируется переходами между различными состояниями. Критерий безопасности модели Харрисона–Руззо–Ульмана формулируется следующим образом – для заданной системы начальное состояние $\mathbf{Q}_o$=($\mathbf{S}_o$, $\mathbf{O}_o$, $\mathbf{M}_o$) является безопасным относительно права *r*, если не существует применимой к $\mathbf{Q}_o$ последовательности команд, в результате которой право *r* будет занесено в ячейку матрицы **M**, в которой оно отсутствовало в состоянии $\mathbf{Q}_o$.

Особо важным для нас является то, что с точки зрения практики построения систем информационной безопасности модель Харрисона-Руззо-Ульмана является наиболее простой в реализации и эффективной в управлении, поскольку не требует никаких сложных алгоритмов и позволяет управлять полномочиями пользователей с точностью до операции над объектом, чем и объясняется ее широкая распространённость среди современных систем. Кроме того, предложенный в данной модели критерий безопасности является весьма сильным в практическом плане, поскольку позволяет гарантировать недоступность определенной информации для пользователей, которым изначально не выданы соответствующие полномочия.

Однако авторы модели доказали, что в общем случае не существует алгоритма, который может для произвольной системы, ее начального состояния $\mathbf{Q}_o$ = ($\mathbf{S}_o$, $\mathbf{O}_o$, $\mathbf{M}_o$) и общего права *r* решить, является ли данная конфигурация безопасной. Таким образом, дискреционная модель Харрисона–Руззо–Ульмана в своей общей постановке не дает гарантий безопасности системы.

Кроме того, все дискреционные модели уязвимы по отношению к атаке с помощью «троянского коня», поскольку в них контролируются только операции доступа субъектов к объектам, а не потоки информации между ними. Данный момент в значительной мере усложняет использование дискреционной модели для систем информационной безопасности, ориентированных на работу в среде интернет/интранет, что как раз и является специфической особенностью веб-ГИС-систем. Еще одним недостатком дискреционной политики доступа является тот факт, что в информационной системе с большим числом объектов и субъектов доступа, таких как ГИС крупного промышленного предприятия, инженерные сети которых содержат десятки тысяч отдельных объектов, администрирование системы является достаточно трудоемкой задачей.

В связи с перечисленными недостатками дискреционных моделей построение на их основе системы информационной безопасности веб-ГИС ведения электронного генерального плана инженерной инфраструктуры будем считать неприемлемым.

Мандатные модели реализуют мандатное управление доступом, которое основано на совокупности правил, определенных на множестве атрибутов безопасности субъектов и объектов. Основой мандатных моделей является модель Белла–ЛаПадулы, базирующаяся на правилах секретного документооборота [2, 3, 6]. Основным положением этой политики безопасности является назначение всем участникам процесса обработки защищаемой информации и документам, в которых она содержится, специальной метки, получившей название уровня безопасности. Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух простых правил:

1) уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности;

2) уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

Таким образом, если в дискреционных моделях управление доступом происходит путем наделения пользователей полномочиями осуществлять определенные операции над определенными объектами, то мандатные модели управляют доступом неявным образом – с помощью назначения всем сущностям системы уровней безопасности, которые определяют все допустимые взаимодействия между ними. Следовательно, мандатное управление доступом не различает сущностей, которым присвоен одинаковый уровень безопасности, и на их взаимодействия ограничения отсутствуют.

Система в модели безопасности Белла-ЛаПадулы [4], как и в модели Харрисона–Руззо–Ульмана, представляется в виде множеств субъектов **S**, объектов **O** и прав доступа read (чтение) и write (запись). Уровни безопасности субъектов и объектов задаются с помощью функции уровня безопасности $\mathbf{F}:\mathbf{S}\cup\mathbf{O}\rightarrow\mathbf{L}$, ставящей в соответствие каждому объекту и субъекту уровень безопасности, принадлежащий множеству уровней безопасности **L**, на котором определена решетка. Для модели Белла–ЛаПадулы существует формальное доказательство безопасности системы, реализующей мандатную политику.

Вместе с тем необходимо отметить трудности, связанные с применением мандатных моделей на практике. Все мандатные модели, как и модель Белла–ЛаПадулы, используют только два права доступа – чтение и запись. На практике информационные системы поддерживают значительно более широкий спектр операций над информацией, например: создание, удаление, передача и т.д. Следовательно, для того чтобы применить мандатную модель к реальной системе, необходимо установить подходящее соответствие между чтением и записью и операциями, реализованными в конкретной системе. Определение такого соответствия представляет собой нетривиальную задачу, поскольку в реальной жизни невозможно ограничиться однонаправленными потоками информации, идущими строго от субъекта к объекту или наоборот.

Поэтому когда в системе используется мандатная политика, все взаимодействия рассматриваются только на достаточно высоком уровне абстракции, на котором не учитываются детали реализации операций доступа.

Кроме того, специфика веб-ГИС для ведения ЭГП предполагает разделение прав и на доступ к функциональному наполнению системы, которое опосредуется задачами субъектов, решаемыми в ходе использования генерального плана, что в явном виде не предусмотрено мандатной моделью.

Таким образом, применение мандатных моделей для управления доступом к объектам веб-ГИС ведения электронного генерального плана инженерной инфраструктуры не оправдано.

Ролевая модель, реализующая ролевую политику безопасности, основана на модели Харрисона–Руззо–Ульмана. Однако ее нельзя отнести ни к дискреционным, ни к мандатным, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов [10].

Классическое понятие «субъект» в ролевой модели замещается понятиями «пользователь» и «роль». Пользователь – это человек, работающий с системой и выполняющий определенные служебные обязанности. Роль – это активно действующая в системе абстрактная сущность, с которой связан ограниченный, логически связанный набор полномочий, необходимых для осуществления определенной деятельности. Данный подход близок к реальной жизни, где пользователи действуют не от своего личного имени, а исполняют определенные служебные обязанности. Поэтому в данной модели управление доступом и назначение полномочий осуществляются не реальным пользователям, а абстрактным ролям, представляющим участников определенного процесса обработки информации, пользователям электронного генерального плана.

При использовании ролевой политики управление доступом осуществляется в две стадии:

1) для каждой роли указывается набор полномочий, представляющий набор прав доступа к объектам;

2) каждому пользователю назначается список доступных ему ролей.

Ролевая модель описывает систему в виде следующих множеств: **U** – множество пользователей; **R** – множество ролей; **P** – множество полномочий на доступ к объектам, представленное, например, в виде матрицы прав доступа; **S** – множество сеансов работы пользователей с системой.

Для перечисленных множеств определяются следующие отношения:

$\mathbf{PA} \subseteq \mathbf{P} \times \mathbf{R}$ – отображает множество полномочий на множество ролей, устанавливая для каждой роли набор присвоенных ей полномочий;

$\mathbf{UA} \subseteq \mathbf{U} \times \mathbf{R}$ – отображает множество пользователей на множество ролей, определяя для каждого пользователя набор доступных ему ролей.

Правила управления доступом ролевой политики безопасности определяются следующими функциями:

user: $\mathbf{S} \to \mathbf{U}$ – для каждого сеанса **S** эта функция определяет пользователя, который осуществляет этот сеанс работы с системой;

roles: $\mathbf{S} \to \{\mathbf{R}\}$ – для каждого сеанса **S** эта функция определяет набор ролей из множества *R*, которые могут быть одновременно доступны пользователю в этом сеансе;

permissions: $\mathbf{S} \to \mathbf{P}$ – для каждого сеанса **S** эта функция задает набор доступных в нем полномочий, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе.

В качестве критерия безопасности ролевой модели используется следующее правило: система считается безопасной, если любой пользователь системы, работающий в сеансе **S**, может осуществлять действия, требующие полномочия **P**, только в том случае, если $\mathbf{P} \in \text{permissions(s)}$. Это означает, что управление доступом осуществляется главным образом не с помощью назначения полномочий ролям, а путем задания отношения **UA** и функции roles.

Ролевая политика безопасности является неотъемлемой частью современных систем управления доступом в корпоративных информационных системах со сложной организационной и штатной структурой, большим количеством пользователей, выполняющих определенные функции в рамках своих служебных обязанностей и наделенных в связи с этим различными правами и полномочиями.

Применение ролевых моделей позволяет существенно упростить проектирование и администрирование систем разграничения доступа автоматизированных информационных систем, реализующих сложные, нетривиальные организационно-технологические и организационно-управленческие схемы и процессы, присущие процессу использования и ведения ЭГП крупного промышленного предприятия [1]. Кроме того, ролевая модель достаточно хорошо отвечает особенностям сервис-ориентированной архитектуры информационных систем, положенной в основу создаваемой веб-ГИС для ведения ЭГП [11].

Заключение. Приведенные выше рассуждения послужили основанием для выбора ролевой модели в качестве формальной основы проектирования и создания системы информационной безопасности веб-ГИС ведения ЭГП.

Использование ролевой модели при проектировании веб-ГИС ведения электронного генерального плана инженерной инфраструктуры позволило спроектировать и создать программное обеспечение по информационной безопасности веб-ориентированной геоинформационной системы обладающее следующими функциональными возможностями:

− Ведение регламента доступа к пространственным данным и функциональной составляющей системы веб-ГИС.

− Организация ролевого регламентированного доступа к данным генерального плана согласно указанным администратором объектам, группам объектов, функциям и территориям.

− Назначение пользователям и их группам права на элементы пользовательского интерфейса Веб-ГИС-клиента: ГИС-слои, информационные отчеты, ГИС-функции.

− Назначение параметров доступа ролям к объектам в двух режимах:

- режим назначения прав через объекты;
- режим назначения прав через роли.

− Определение пользователя как члена группы.

− Определение прав членов группы на доступ к пространственным данным по набору слоев, по указанной области территории генплана, по типу объектов инженерной сети.

− Определение прав членов группы на доступ к технологическим возможностям системы, представленным как функции веб-ГИС-клиента.

Материалы данной статьи разрабатывались при финансовой поддержке Министерства образования и науки Российской Федерации в рамках мероприятия 2.4 федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007–2013 годы», государственного контракта № 07.524.11.4013.

Литература

1. Гриценко Ю.Б. Геоинформационные технологии мониторинга инженерных сетей / Ю.Б. Гриценко, Ю.П. Ехлаков, О.И. Жуковский. – Томск: Изд-во Том. гос. ун-та систем управления и радиоэлектроники, 2010. – 148 с.

2. Зегжда Д.П. Принципы и методы создания защищенных систем обработки информации: дис. ... д-ра техн. наук : 05.13.19. – СПб., 2002. – 380 с.

3. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд-во Урал. ун-та, 2003. – 328 с.

4. Ferraiolo D.F. Introduced formal model for role based access control / D.F. Ferraiolo, D.R. Kuhn // Role Based Access Control 15th National Computer Security Conference, Oct 13-16, 1992. – P. 554–563. [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/groups/SNS/rbac/documents/Role_Based_Access_Control-1992.html, свободный (дата обращения: 24.10.2012).

5. ISO/IEC 17799:2000 «Information technology – Information security management» [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33441, свободный (дата обращения: 10.09.2012).

6. LaPadula L.J. Elliott Secure Computer Systems: A Mathematical Model / Leonard J. LaPadula, D. Bell // MITRE Corporation Technical Report 2547, V. II. 31 May 1973 [Электронный ресурс]. – Режим доступа: http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf, свободный (дата обращения: 10.09.2012).

7. McLean John. Security models // Encyclopedia of software engineering, 1994 [Электронный ресурс]. – Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.34.8561, свободный (дата обращения: 10.09.2012).

8. McLean John. The Specification and Modeling of Computer Security // Computer, 23(1): 9-16, January 1990. – P. 9–16. – Режим доступа: http://users.cis.fiu.edu/~nemo/cot6930/mclean90specification.pdf, свободный (дата обращения: 24.10.2012).

9. Harrison M. Monotonic protection systems / M. Harrison, W. Ruzzo // Foundation of secure computation. – N.Y.: Academic Press, 1978. – P. 337–363.

10. Sandhu Ravi S. The Typed Access Matrix Model // Proceedings of IEEE Symposium on Security and Privacy. – Oakland, California, 1992. – P. 122–136.

11. Жуковский О.И. Применение стилей сервис-ориентированной архитектуры для разработки геоинформационных систем / О.И. Жуковский, Н.Б. Рыбалов, С.С. Ощепков // Научно-технические ведомости СПбГУ. – 2009. – № 1. – С. 16–21.

Жуковский Олег Игоревич
Канд. техн. наук, доцент каф. АОИ ТУСУРа
Тел.: (382-2) 70-15-46
Эл. почта: ol@muma.tusur.ru

Гриценко Юрий Борисович
Канд. техн. наук, доцент каф. АОИ ТУСУРа
Тел.: (382-2) 70-15-46
Эл. почта: ubg@muma.tusur.ru

Zhukovsky O.I., Gritsenko Yu.B.
Choice of access models for Web GIS conducting electronic engineering infrastructure master plan

The paper presents the problem of choosing the model of access to web-GIS master plan for conducting electronic business. The basic access model is used in the design and development of modern automated systems in large industrial plants. We present the possibilities of information security in Web GIS system of electronic master plan, developed on the basis of one of the access models.
Keywords: electronic master plan, engineering infrastructure, access model, role model.