УДК 004.056

Розенберг И.Н., Булгаков С.В.

ПРОЕКТНАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГИС*

Аннотация. В статье описана проектная модель информационной безопасности. Проводится ее сравнение с другими моделями. Показаны особенности и отличия предлагаемой новой модели.

Ключевые слова: геоинформатика, информационная безопасность, моделирование.

Особенностью информационной безопасности ГИС является ее повышенная уязвимость. Это обусловлено большим числом каналов получения данных и каналами обмена информации [1]. Для отражения внешних угроз и обеспечения информационной безопасности различных систем, включая информационные, применяют разные модели защит, которые отражают разные концепции, заложенные в этих моделях. Краткий перечень основных моделей следующий [2]: модель Биба, модель Гогена-Мезингера, Сазерлендская модель и модель Кларка-Вильсона.

Модель Биба - (1977) основана на классификации и идентификации всех субъектов и объектов; разделение субъектов и объектов по уровням доступа; наложением на их идентификаторы ограничений.

Модель Гогена-Мезингера (1982) основана на теории автоматов. В соответствии с данной моделью определены допустимые состояния для системы. Система может переходить из одного разрешенного состояния в другие. Субъекты и объекты разбиты на группы; переход системы из одного состояния в другое выполняется в соответствии с таблицей разрешений, в которой указано, какие операции может выполнять субъект; переход из одного состояния в другое осуществляется с использованием транзакций, что обеспечивает общую целостность системы.

Эта модель существенно повторяет предыдущую модель. Отличие во введении разрешенных состояний системы. Однако это накладывает и ограничение для самоуправляющихся и самоорганизующихся систему

Сазерлендская модель (1986) основана на морфизме субъектов и потоков информации. В этой модели используется машина состояний со множеством разрешенных комбинаций состояний и некоторым набором начальных позиций. При этом исследованию и контролю подлежит поведение множественных композиций функций перехода из одного состояния в другое. Эта модель дополняет предыдущую множество комбинаций состояний.

Модель Кларка-Вильсона (1989) основана на рассмотрении взаимодействий системы как транзакций и тщательном оформлении прав доступа субъектов к объектам. Информационные взаимодействия описываются через транзакции, что повышает их защищенность. В этой модели впервые исследована защищенность третьей стороны, поддерживающей всю систему безопасности (программы-супервизора). Кроме того, в данной модели идентификация субъекта производится, перед выполнением команды от него, но и повторно после выполнения.

Общий недостаток всех рассмотренных моделей – апостериорный подход. Они защищают информационные системы после их создания. Для устранения этого недостатка и в развитии идей модели Кларка-Вильсона авторами работы предложена модель проектной защиты.

Идея модели Кларка-Вильсона о защищенность третьей стороны, поддерживающей всю систему безопасности *в процессе работы системы*, трансформирована в идею защиты компьютерной среды, инфраструктуры информационных систем в ней и самих ИС на этапе создания *компьютерной среды* (КС) и последующей конфигурации инфраструктуры и самой системы *до начала работы* системы. Принципиальным отличием данной модели является создание системы защиты до установки системы. Другим отличием является то, что в качестве объекта защиты рассматривается не изолированная ГИС, а компьютерная среда плюс инфраструктура ГИС (ИИГИС), плюс сама ГИС. Отличие в периоде создания и широте защиты. По существу этап защиты встраивается в начальный этап проектирования компьютерной среды и системы, поэтому такая модель названа проектной моделью защиты информации (ПМЗИ).

При построении этой модели защиты учитывается предположение о том, что понятие информационной безопасности КС+ИИГИС шире, чем понятие безопасности ИС или ГИС. Это приводит к необходимости включения в ПМЗИ дополнительных параметров и показателей, отражающих защищенность компьютерной среды. К таковым относятся не только защищенность, но и качество проектирования, среды, надежность функционирования и др.

Можно выделить четыре группы функций КС + ИИГИС в аспекте безопасности. Первая группа (группа проектирования) содержит функции проектирования и организации системы. Вторая группа функций (нормального функционирования) обеспечивает надежность функционирования, третья (отражения угроз) выполнение обнаружения и минимизации угроз. Четвертая группа функций (ликвидации последствий деструктивных воздействий) обеспечивает минимизацию ущерба от последствий деструктивного воздействия.

В совокупности все эти функции обеспечивают безопасность IIS на всех стадиях жизненного цикла. Вектор угроз (VT) воздействует на структурную матрицу системы (СМС) и приводит к деструктивным воздействиям (DR).

$$СМС \times VT = DR$$

Необходимо минимизировать DR. Это возможно если усилить все компоненты структуры, которые включают КС + ИИГИС +ГИС. Это определяет необходимость усиления этого комплекса на этапе проектирования. Отсюда следует, что ПМЗИ является наиболее стойкой к внешним угрозам. Построение ПМЗИ включают следующие этапы

1. Проектирование дискового пространства в соответствии с типами и видами данных, а также баз данных и программных средств.
2. Установка брандмауера
3. Установка антивируса с функцией анитиспама.
4. Альтернатива пп.2-3 установка программного комплекса типа Интернет-Секьюрети
5. Конфигурирование данных. Расположение данных на разных дисках или разных разделах с ПО ОС
6. Проектирование шифрования архивных данных (геоданных) с сохранением ключа на резервном носителе.
7. Установка пароля на вход.
8. Установка пароля на хранитель экрана
9. Установка ПО резервного копирования
10. Установка ПО контроля состояния жестких дисков с технологией SMART.

Таким образом, данный подход повышает надежность и защищенность ГИС, инф-

раструктуры ГИС и компьютерной среды за счет более четкой организации информационных процессов и конфигурации информационного пространства на компьютере.

СПИСОК ЛИТЕРАТУРЫ:

1. Иванников А.Д., Кулагин В.П., Тихонов А.Н. . Цветков В.Я. Информационная безопасность в геоинформатике. - М.: МаксПресс 2004 -336 с.
2. Майоров А.А., Цветков В.Я. Хранение и защита информационных ресурсов кадастра. – М.: Московский государственный университет геодезии и картографии, 2009. – 126 с.

I. Rosenberg, S. Bulgakov

DESIGN MODEL OF INFORMATION SAFETY GIS

Abstract. In the paper the design model of information safety is described. Its comparison with other models is spent. Features and differences of offered new model are shown

Key words: geoinformatics, information safety, modelling.