УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Факультет ИРТ

Кафедра ВТиЗИ

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**К КУРСОВОЙ РАБОТЕ**

**по дисциплине**

**"Теория информационной безопасности и методология защиты информации"**

**НА ТЕМУ:\_IDEF–моделирование мандатного (полномочного) разграничения доступа**

Выполнил: студ. Миргалеев И.В.. гр. ЗИ-322 .

Консультант: к.т.н, доцент Агзамов З.В. .

ученая степень, ученое звание, должность

Проверил: к.т.н, доцент Агзамов З.В. .

ученая степень, ученое звание, должность

Оценка:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Уфа 2007

УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ

ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

**КАЛЕНДАРНЫЙ ПЛАН**

**курсовой работы**

студента:\_\_\_\_\_\_\_\_\_\_\_группы ЗИ-322 Миргалеева И.В.\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Тема работы \_\_\_«IDEF–моделирование мандатного (полномочного) разграничения доступа»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Наименование этапов курсовой работы | Срок | Объем от всей работы в % | Фактическое |
| 1 | Утверждение темы курсовой работы. Анализ технического задания. | неделя | 10 | 10 |
|  | Поиск материалов в Интернете, перевод наиболее интересных статей | неделя | 30 | 30 |
| 3 | Разработка функциональной модели | неделя | 25 | 25 |
| 4 | Разработка информационной модели | неделя | 20 | 20 |
| 6 | Оформление пояснительной записки. Подготовка к защите курсовой работы | неделя | 15 | 15 |

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, дата)

Руководитель работы\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, дата)

**Реферат**

В ходе выполнения данной курсовой работы была разработана модель разграничения доступа мандатного (полномочного) типа. Курсовая работа содержит 27 страниц, 17 рисунков.

В работе рассматривается мандатная (полномочная) система разграничения доступом. Суть ее такова, что в СЗИ вводятся уровни безопасности, или иначе уровни секретности. Работники с самым высоким уровнем безопасности могут работать с документами самой высокой степени секретности.

В качестве среды моделирования использовалась программа Design/IDEF 3.5. Посредством этой программы были разработаны функциональная и информационная модели проектируемой системы разграничения доступа мандатного (полномочного) типа. Для динамического моделирования использовалась программа построения сетей Петри Graf.

**Содержание**

Введение

1 Описание системы мандатного разграничения доступа

2 Разработка функциональной модели

2.1 Первый уровень функциональной модели

2.2 Второй уровень функциональной модели

2.3 Третий уровень функциональной модели

2.4 Четвертый уровень функциональной модели

2.5 Пятый уровень функциональной модели

3 Разработка информационной модели

4 Разработка динамической модели

Заключение

Список использованной литературы

## Введение

Необходимость использования механизмов для разграничения прав доступа возникла довольно давно. В любой компьютерной системе, которая предоставляется для множества пользователей, необходимо тщательно продумать политику безопасности для обеспечения трех основных концепций защиты информации:

- конфиденциальность информации,

- целостность информации,

- доступность информации;

Основу для установки, анализа и применения политик безопасности в многопользовательских системах предоставляют модели контроля доступа. Обычно эти модели определяются в терминах известных обобщений субъектов, объектов и прав доступа.

Разграничив области доступа можно значительно снизить вероятность ошибок операторов. Система разграничения доступа - совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах. Средства логического разграничения доступа определяют действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информационными ресурсами, процессами, устройствами и т. п.). Такие средства позволяют также обеспечить контроль (поддерживают режим протоколирования) за совершением этих действий. В отличие от физического управления доступом, которое осуществляется на операционном уровне, например, персоналом, регламентирующим доступ пользователя в специальные помещения (компьютерные классы), в данном случае имеется в виду доступ, который обеспечивается программно-техническими средствами.

**1 Описание системы мандатного разграничения доступа**

Исходным толчком к разработке мандатной политики послужили проблемы с контролем распространения прав доступа, и, в особенности, проблема «троянских» программ в системах с дискреционным доступом. Исследователи и критики дискреционной политики, понимая, что основная проблема дискреционных моделей заключается в отсутствии контроля за информационными потоками, проанализировали, каким образом подобные проблемы решаются в секретном делопроизводстве.

Было отмечено следующее:

1. Разграничение доступа и порядок работы с конфиденциальными «бумажными» документами организуется на основе парадигмы градации доверия определенным группам работников в отношении государственных секретов определенной степени важности. С этой целью вводиться система уровней безопасности, или иначе уровней секретности. Работники с самым высоким уровнем безопасности (уровнем доверия), могут работать с документами самой высокой степени секретности. На более низком уровне доверия, т.е. на более низком уровне безопасности, вводятся ограничения в отношении работы с документами более высокой степени секретности и т.д. Соответственно, все работники получают так называемый допуск к работе с секретными документами определенного уровня, а документы снабжаются определенной меткой, отражающей требования к уровню безопасности при работе с ними, - так называемы гриф секретности.
2. Критерием безопасности является невозможность получение информации из документов определенного уровня безопасности работником, чей уровень безопасности, т.е. уровень доверия, ниже, чем уровень безопасности соответствующих документов.

Данный критерий безопасности фактически означает запрет определенных информационных потоков, которые трактуются как опасные или недопустимые.

Кроме того, были проанализированы правила и система назначений, изменений, лишений и т.д. допусков сотрудников к работе с секретными документами, правила создания, уничтожения документов, присвоения или изменения грифов их секретности, в том числе и рассекречивания, а также другие особенности работы с секретными документами. В частности было отмечено, что получения доступа к документам различаются в зависимости от характера работы с ними – изучение (чтение) или изменение (создание, уничтожение, внесение дополнений, редактирование, т.е. запись в них). На этой основе было выявлено два основных правила, гарантирующих безопасность:

Правило 1 (no read up (NRU) – нет чтения вверх). Работник не имеет права знакомиться с документом (читать), гриф секретности (уровень безопасности) которого выше его степени допуска (уровня безопасности).

Правило 2 (no write down (NWD) – нет записи вниз). Работник не имеет права вносить информацию (писать) своего уровня безопасности в документ с более низким уровнем безопасности (с более низким грифом секретности).

Первое правило является естественным и очевидным способом обеспечения безопасности при осуществлении информационных потоков из документов к работникам и иначе может быть сформулировано так: - работнику нельзя получать информацию, уровень секретности которой выше его уровня доверия. Второе правило обеспечивает безопасность при осуществлении информационных потоков от работника к документу и иначе может быть сформулировано так: - работнику нельзя передавать информацию своего уровня секретности в тех случаях, когда в результате передачи с ней могут ознакомиться работники с более низким уровнем безопасности.

Формализация данных механизмов разграничения доступа в секретном делопроизводстве применительно к субъектно-объектой модели компьютерной системы показала необходимость решения ряда следующих задач:

- разработка процедур формализации правила NRU, и в особенности правила NWD;

- построение формального математического объекта и процедур, адекватно отражающих систему уровней безопасности (систему допусков и грифов секретности).

Нетрудно увидеть, что при представлении работников, работающих с секретными документами, субъектами доступа, а секретных документов в качестве объектов доступа компьютерной системы, буквальное следование правилу NWD приводит к автоматическому включению в механизмы обеспечения безопасности субъективного фактора в лице субъекта-пользователя, который при внесении информации в объекты-документы, с более низким грифом секретности должен субъективно оценить соответствие вносимой информации уровню безопасности документа. Задача исключения данного субъективного фактора может решаться различными способами, самым простым из которых является полный запрет изменения субъектами (доступ write) объектов с уровнем безопасности, более низким, чем уровень безопасности соответствующих субъектов.

При этом, однако, помимо существенного снижения функциональности компьютерной системы, логика такого запрета, автоматически приводит к «не запрету» (т.е. к разрешению) возможностей изменения объектов-документов с более высоким уровнем безопасности, чем уровень безопасности соответствующих субъектов-пользователей. Действительно, внесение информации более низкого уровня секретности в объекты с более высоким уровнем секретности не может привести к нарушению безопасности системы в смысле рассмотренного выше критерия безопасности.

В качестве основы для решения второй задачи при создании моделей мандатного доступа был использован аппарат математических решеток.

Введем следующие определения.

Определение 1. Решеткой уровней безопасности AL называется формальная алгебра AL(L, ≤, •, ),



где L – базовое множество уровней безопасности;

≤ - оператор, который определяет частичное нестрогое отношение порядка для элементов множества L, обладающее свойствами антисимметричности, транзитивности и рефлективности:

(рефлективность);



(антисимметричность);



(транзитивность).



• - оператор, задающий для любой пары элементов множества L единственный элемент наименьшей верхней границы:



- оператор, задающий для любой пары элементов множества L наибольшей нижней границы:



Определение 2. Функцией уровня безопасности FL:X→L называется однозначное отображения множества сущностей компьютерной системы X=SO во множество уровней безопасности L решетки AL.



Обратное отображение FL-1:L→X задает разделение всех сущностей компьютерное системы на классы безопасности такие, что:



где N – мощность базового множества уровней безопасности L;

где



где



Покажем, что введенная решетка и функция уровней безопасности адекватно отражают парадигму градуированного доверия и критерий безопасности систем на ее основе.

1. Предположим, что информация может передаваться от сущностей класса к сущностям класса и наоборот, т.е. от сущности класса к сущностям класса . Тогда для выполнения критерия безопасности сущности классов и должны образовывать один общий класс . Для того, чтобы не создавать избыточных классов, необходимо, чтобы отношение, задаваемое оператором доминирования , было антисимметричным.



1. Предположим, что информация может передаваться от сущностей класса к сущностям класса , и, кроме того, от сущностей класса к сущностям класса . Если каждая такая передача безопасна в отдельности, то, очевидно, безопасна и передача информации от сущностей класса к сущностям класса . Таким образом, отношение, задаваемое оператором , должно быть транзитивным.



1. Внутри класса сущности имеют одинаковый уровень безопасности. Следовательно, передача информации между сущностями одного класса безопасна. Отсюда следует сравнимость по оператору сущностей одного класса между собой и самих собой, т.е. рефлективность отношения .



1. Предположим, что имеется два различных класса сущностей и . Тогда, из соображений безопасности, очевидно, что существует только один класс , потоки от сущностей которого безопасны по отношению к сущностям класса или класса , совпадающий с классом или с классом , и не имеется никакого другого класса , менее безопасного чем , и с такими же возможностями по потокам к сущностям классов и . Это означает, что должен быть наименьшей верхней границей по уровням безопасности классов и .



1. Аналогично по условиям предыдущего пункта должен существовать ближайший снизу к классам и класс , такой, что потоки от сущностей классов и к сущностям класса безопасны, и совпадающий с классом или с классом , при этом не имеется никакого другого класса , более безопасного, чем , и с такими же возможностями по потокам от сущностей классов и . Это означает, что должен быть наибольшей нижней границей по уровням безопасности классов и .



Таким образом, аппарат решетки и функция уровней безопасности адекватно отражают сущность принципов и отношений политики мандатного разграничения доступа, на базе которых строятся конкретные модели, специфицирующие, в том числе, формализацию правил NRU и NWD, а также другие особенности мандатного доступа.

В заключение общей характеристики политики мандатного доступа отметим, что в ней разграничение доступа осуществляется до уровня классов безопасности сущностей системы. Иначе говоря, любой объект определенного уровня безопасности доступен любому субъекту соответствующего уровня безопасности (с учетом правил NRU и NWD). Нетрудно видеть, что мандатный подход к разграничению доступа, основываясь только лишь на идеологии градуированного доверия, без учета специфики характеристик субъектов и объектов, приводит в большинстве случаев к избыточности прав доступа для конкретных субъектов в пределах соответствующих классов безопасности, что противоречит самому понятию разграничения доступа. Для устранения данного недостатка мандатный принцип доступа дополняется дискреционным внутри соответствующих классов безопасности. В теоретических моделях для этого вводят матрицу доступа, разграничивающую разрешенный по мандатному принципу доступ к объектам одного уровня безопасности.

**2 Разработка функциональной модели**

Методология IDEFO (более известная как методологий SADT — Structure Analysis and Design Technique) предназначена для представления функций системы и анализа требований к системам и является одной из самых известных и широко используемых методологий проектирования АСУ.

В терминах IDEFO система представляется в виде комбинации блоков и дуг. Блоки используются для представления функций системы и сопровождаются текстами на естественном языке.

Кроме функциональных блоков другим ключевым элементом методологии является дуга. Дуги представляют множества объектов (как физических, так и информационных) или действия, которые образуют связи между функциональными блоками.

Место соединения дуги с блоком определяет тип интерфейса. Данные, управляющие выполнением функции, входят в блок сверху, в то время как информация, которая подвергается воздействию функции, показана с левой стороны блока; результаты выхода показаны с правой стороны. Механизм (человек или автоматизированная система), который осуществляет функцию, представляется дугой, входящей в блок снизу.

Функциональный блок (или Функция) преобразует Входы в Выходы (т.е. входную информацию в выходную). Управление определяет, когда и как это преобразование может, или должно произойти. Исполнители непосредственно осуществляют это преобразование.

С дугами связаны надписи (или метки) на естественном языке, описывающие данные, которые они представляют. Дуги показывают, как функции между собой взаимосвязаны, как они обмениваются данными и осуществляют управление друг другом. Выходы одной функции могут быть Входами, Управлением или Исполнителями для другой.

Дуги могут разветвляться и соединяться.

Функциональный блок, который представляет систему в качестве единого модуля, детализируется на другой диаграмме с помощью нескольких блоков, соединенных между собой интерфейсными дугами. Эти блоки представляют основные подфункции (подмодули) единого исходного модуля. Данная декомпозиция выявляет полный набор подмодулей, каждый из которых представлен как блок, границы которого определены интерфейсными дугами. Каждый из этих подмодулей может быть декомпозирован подобным же образом для более детального представления.

Рассмотрим построение функциональной модели применительно к моей модели разграничения доступа.

**2.1 Первый уровень функциональной модели**

На входе функционального блока «Разграничение доступа» (А0) – «параметры пользователя», необходимая для последующего ее преобразования, на выходе – «отказ в запросе» и «выполнение запроса» (см. рисунок 1). Результат «отказ в запросе» может появиться в случае невыполнения каких-либо необходимых условий и требований. Управляющее воздействие, в данной модели, - это «монитор безопасности». Механизмом, который осуществляет данную функцию, является компьютерная система.



Рисунок 1 – Первый уровень

Как уже выше было сказано, функциональный блок, который представляет систему в качестве единого модуля, детализируется на другой диаграмме с помощью нескольких блоков, соединенных между собой интерфейсными дугами. Эти блоки представляют основные подфункции (подмодули) единого исходного модуля. Следовательно, можно рассмотреть второй уровень модели, детализирующий первый.

**2.2 Второй уровень функциональной модели**

Второй уровень раскрывает первый, «разграничение доступа» состоит из нескольких следующих этапов:

- идентификация пользователя, который подает запрос (А1);

- анализ запроса, включающий в себя ряд функциональных операций по обработке запроса и осуществляющий функцию разграничения доступа (А2);



Рисунок 2- Второй уровень. Детализация блока А0

**2.3 Третий уровень функциональной модели**

Третий уровень раскрывает все блоки второго уровня. Рассмотрим их поочередно:

* Блок А1 (Идентификация пользователя) включает в себя:

а) Ввод идентификационных данных (А11);

б) Проверка идентификационных данных (А12);

в) Анализ идентификационных данных (А13).

Если на одном из этапов произошло не выполнение каких-либо требований, то система оповещает о том, что в данном случае в запросе отказано.



Рисунок 3 – Третий уровень. Детализация блока А1

- Блок А2 (Анализ запроса) включает в себя:

а) ввод запроса (А21);

б) определение вида и обработка запроса (А22).



Рисунок 4 – Третий уровень. Детализация блока А2

**2.4 Четвертый уровень функциональной модели**

* Блок А13(Анализ идентификационных данных) изображен на рисунке 5 и включает в себя:

а) определение прав в матрице доступа (А131);

б) определение уровня доверия пользователю (А132).



Рисунок 5 – Четвертый уровень. Детализация А13

* Блок А22 (определение вида и обработка запроса) включает в себя:

а) определение вида запроса (А221);

б) выборка запроса из множества запросов (А225);

в) определение уровня защиты объекта (А224);

г) проверка на наличие опасных информационных потоков (А222);

д) проверка соблюдения правил NRU и NWD;

е) проверка наличия соответствующих прав доступа в матрице доступа.



Рисунок 6 – Четвертый уровень. Детализация А22

**2.4 Пятый уровень функциональной модели**

- Блок А222 (Проверка на наличие опасных информационных потоков) включает в себя:

а) проверка на наличие полученных доступов (А2241);

б) определение уровней защиты объектов, к которым получен доступ (А2242);

в) проверка на недопустимые информационные потоки (А2243).



Рисунок 7 – Пятый уровень. Детализация А222

- Блок А223 (Проверка правил NRU и NWD) включает в себя:

а) проверка правила NWD (А2231);

б) проверка правила NRU (А2232).



Рисунок 8 – Пятый уровень. Детализация А223

**3 Разработка информационной модели**

Цель информационной модели заключается в выработке непротиворечивой интерпретации данных и взаимосвязей между ними, что необходимо для интеграции, совместного использования и управления целостностью данных.

Методология IDEF1X - один из подходов к семантическому моделированию данных (определению значений данных в контексте их взаимосвязей с другими данными), основанный на концепции Сущность-Отношение. Это инструмент используется для анализа информационной структуры систем различной природы. Информационная модель, построенная с помощью IDEFlX- методологии, представляет логическую структуру информации об объектах системы. Эта информация является необходимым дополнением функциональной IDEFO- модели поскольку детализирует объекты, которыми манипулируют функции системы.

Основными компонентами IDEF1X- модели являются:

- Сущности, представляющие множество реальных или абстрактных предметов (людей, объектов, мест, событий, состояний, идей, пар предметов и т.д). Они изображаются блоками. Могут быть:

* независимые от идентификатора сущности;
* зависимые от идентификатора сущности.

- Отношения между этими предметами, изображаемые соединяющими блоки линиями. Могут быть:

* отношения, идентифицирующие связи;
* отношения, не идентифицирующие связи;
* отношения категоризации;
* неспецифические отношения.

- Характеристики сущностей, изображаемые именами атрибутов внутри блоков. Атрибуты могут быть:

* неключевыми;
* первичными ключами;
* альтернативными ключами;
* внешними ключами.

Сущность – это совокупность похожих объектов/экземпляров (людей, мест, предметов, событий), которая именуется общим существительным, обладает ключом (однозначно идентифицирующим каждый экземпляр) и имеет один или несколько атрибутов (описывающих каждый экземпляр).

Каждая сущность может обладать любым количеством отношений с другими сущностями. Сущность является независимой, если каждый экземпляр сущности может быть однозначно идентифицирован без определения его отношений с другими сущностями. Независимая сущность на диаграмме изображается блоком с прямыми углами. Сущность называется зависимой, если однозначная идентификация экземпляра сущности зависит от его отношения к другой сущности. Если сущность зависима от идентификатора, то углы блока закругляются.

Отношение связи, называемое также отношением родитель-потомок, - это связь между сущностями, при которой каждый экземпляр сущности-родитель ассоциирован с произвольным (в том числе нулевым) количеством экземпляров сущности-потомком, а - каждый экземпляр сущности-потомка ассоциирован в точности с одним экземпляром сущности-родителя.

Идентифицирующим отношением называется отношение, при котором экземпляр сущности-потомка однозначно определяется своей связью с сущностью-родителем. В противном случае отношение называется неидентифицирующим. Идентифицирующее отношение изображается сплошной линией, пунктирная линия изображает неидентифицирующее отношение.

Отношению дается имя, выражаемое грамматическим оборотом глагола. Имя отношения всегда формируется с точки зрения родителя, так что может быть образовано предложение, если соединить имя сущности-родителя, имя отношения, выражение мощности и имя сущности-потомка.

Каждый экземпляр общей сущности и связанный с ним экземпляр одной из категорных сущностей изображают один и тот же предмет реального мира и поэтому обладают одним и тем же уникальным идентификатором. Для сущности-категории мощность не указывается, поскольку она всегда равна нулю или единице. Значение некоторого атрибута в экземпляре общей сущности определяет, с каким из возможных сущностей-категорий он связан. Этот атрибут называется дискриминатором отношения категоризации.

Рассмотрим информационную модель применительно к рассматриваемой мною модели мандатного разграничения доступа. Информационная модель дает логическую схему проектируемой модели. Сущность «Разграничение доступа» в информационной модели (см. рисунок 9 и 10) связана с 2 другими сущностями («идентификация пользователя» и «анализ запроса») с помощью отношения «состоит». Эти две сущности также имеют отношения «включает» с рядом других сущностей, то есть модификация матрицы происходит только при выполнении всех этих функций. Ниже приведены диаграммы информационной модели для разработанной ранее функциональной модели.



Рисунок 9 – Информационная модель. Идентификация пользователя



Рисунок 10 – Информационная модель. Анализ запроса

**4 Динамическая модель**

В общем виде сети Петри позволяют построить модели сложных систем в виде соответствующих структур, образованных из элементов двух типов - событий и условий. В свою очередь в сетях события и условия представлены в виде двух непересекающихся множеств, а именно множеством позиций и множеством переходов. В графическом представлении сетей переходы представляются "барьерами", а позиции – кружками. Динамика поведения моделируемой системы отражается в функционировании сети и виде совокупности локальных действий, которые называются срабатываниями переходов. Они соответствуют реализациям событий и приводят к изменению разметки позиций, т.е. к локальному изменению условий в системе. Переход может сработать, если выполнены все условия реализации соответствующего события.

Рассмотрим динамическую модель применительно к моей модели разграничения доступа мандатного типа. На рисунке 11 представлен общий вид модели и объяснены назначения переходов.

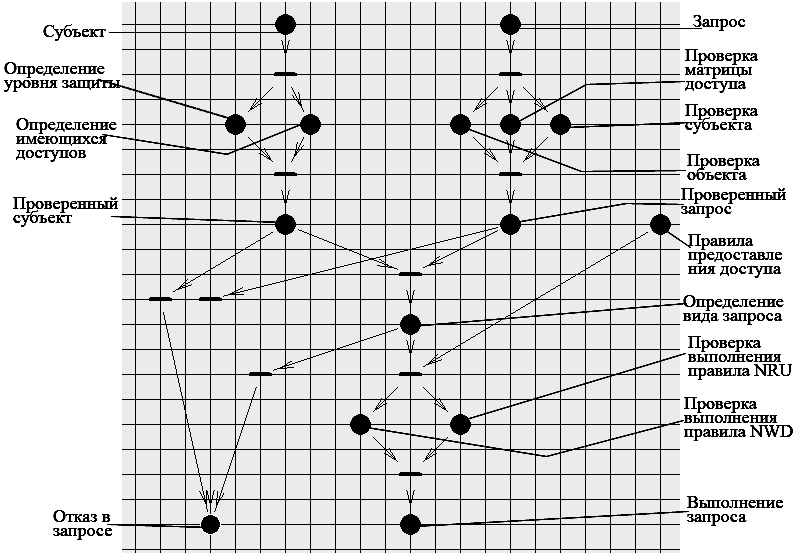


Рисунок 11 – Общий вид динамической модели

Матрица может быть модифицирована при выполнении трех условий:

* наличие проверенного субъекта;
* наличие проверенного запроса;
* выполнение правил предоставления доступа.

Рассмотрим случай, когда запрос может быть предоставлен. Для этого необходимо, чтобы метка была установлена в трех кружочках: «Субъект», «Запрос» и «Правила предоставления доступа» (см. рисунок 12а).

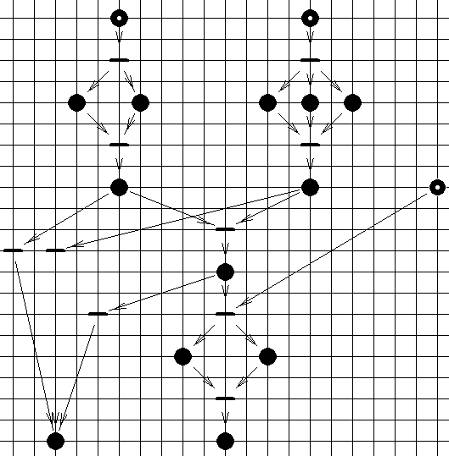


Рисунок 12а – Первоначальное состояние динамической модели

Если данное условие выполняется, то при запуске системы, метка переместится в нижний правый кружочек, что соответствует состоянию «Выполнение запроса» (см. рисунок 12б).

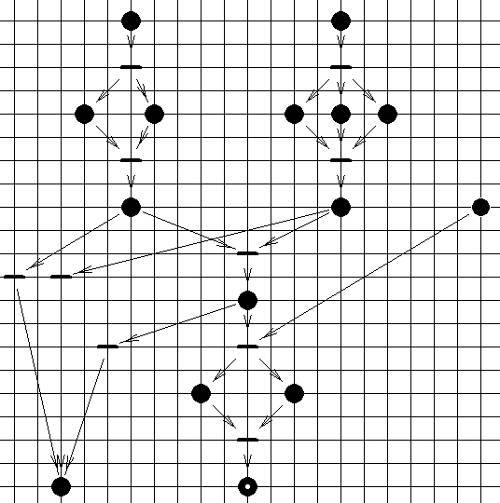


Рисунок 12б – Конечное состояние динамической модели. Запрос выполнен

Если же одно из этих условий не выполняется, например, «Правила предоставления доступа», то начальное положение системы будет соответствовать наличию меток только к кружочках «Субъект», «Запрос» и отсутствию в кружочке «Правила предоставления доступа» (см. рисунок 13а). Конечное же состояние будет соответствовать наличию метки в кружочке «Отказ в запросе» (см. рисунок 13б).

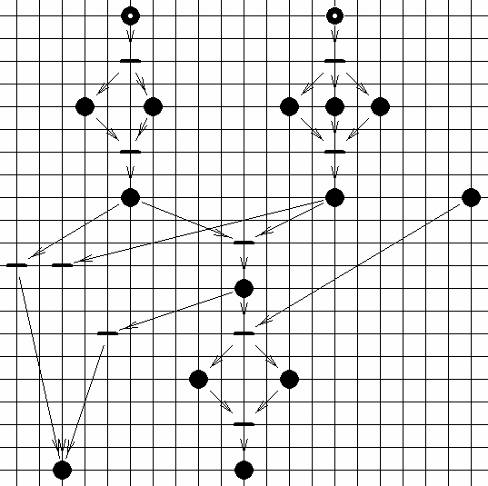


Рисунок 13а – Первоначальное состояние системы.

Отсутствует необходимая метка

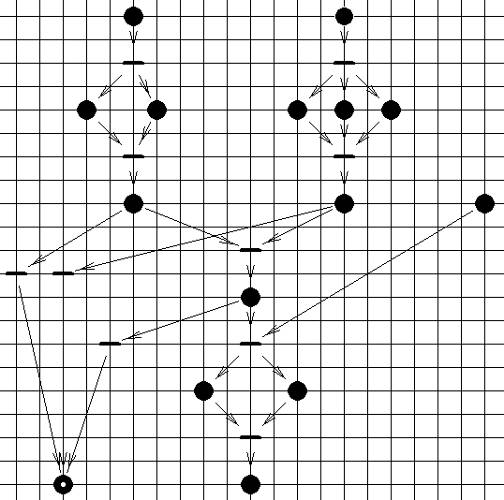


Рисунок 13б – Конечное состояние системы.

В запросе отказано

Если в начальном положений будет отсутствовать метка в кружочке «Субъект» или «Запрос» (см. рисунок 14а), то конечное состояние также будет соответствовать метки в кружочке «Отказ в запросе» (см. рисунок 14б).

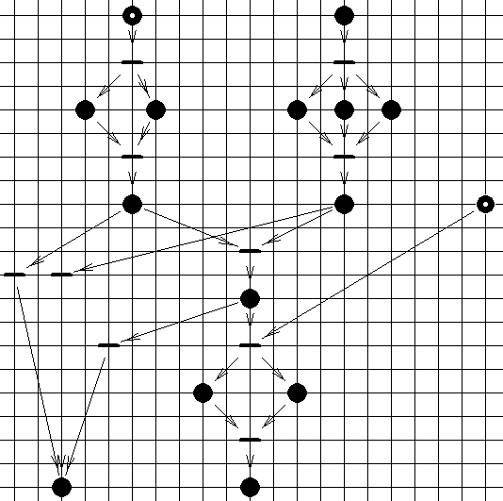


Рисунок 14а – Начальное состояние системы.

Отсутствует необходимая метка

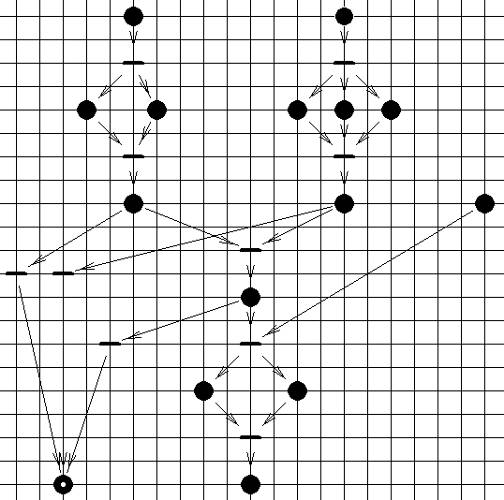


Рисунок 14б – Конечное состояние системы.

В запросе отказано

**Заключение**

При выполнении данного курсового проекта были изучены материалы по модели мандатного (полномочного) разграничения доступа, рассмотрены принципы предоставления доступа, реализуемые в данной модели. И на их основе разработаны функциональная, информационная и динамическая IDEF-модели разграничения доступа. При этом использовалась программа Design/Idef 3.5 и Graf, реализующая сети Петри. По ходу курсового проектирования были изучены материалы по стандарту SADT.

**Список использованной литературы**

1. Методические указания к курсовой работе по дисциплине "Теория информационной безопасности и методология защиты информации" /Уфимск. гос. авиац. техн. ун-т; Cост. З.В. Агзамов; — Уфа, 2004.

2. Методические указания к лабораторным работам по курсу "Кибернетические основы информационных систем" для студентов направления 552800 "Информатика и вычислительная техника" и 552300 "Информационные системы в экономике"/Уфимск.гос.авиац. техн. ун-т; Сост. Г. Г. Куликов, А. Н. Набатов. Уфа, 1995.- 35 с.

3. Куликов Г.Г. Набатов А.Н. Речкалов А.В. Автоматизированное проектирование информационно-управляющих систем. Проектирование экспертных систем на основе системного моделирования – УГАТУ Уфа 1997.

4. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах, 2003.