



**ВОРОНЕЖСКИЙ ИНСТИТУТ ВЫСОКИХ ТЕХНОЛОГИЙ – АНОО ВПО**  
**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ЛАБОРАТОРНЫХ РАБОТ**

**По дисциплине «Защита информации»**

**Лабораторная работа № 4**

**«РЕАЛИЗАЦИЯ МАНДАТНОЙ МОДЕЛИ ПОЛИТИКИ БЕЗОПАСНОСТИ»**

**Цель** – познакомиться с проблемами реализации политик безопасности в компьютерных системах на примере мандатной модели.

**Теоретический материал**

Мандатная модель политики безопасности предполагает нормативное управление доступом субъектов к объектам с использованием меток безопасности.

В данной модели каждому субъекту приписывается уровень допуска (форма допуска), а каждому объекту – уровень конфиденциальности (гриф секретности).

Мандатную модель можно определить следующей группой аксиом:

1. Имеется множество атрибутов безопасности. В качестве таких атрибутов достаточно часто используется следующее множество: {«Совершенно секретно», «Секретно», «Открытые данные»}.

2. Каждому объекту компьютерной системы присваивается определенный атрибут безопасности, который соответствует его ценности.

3. Каждому субъекту присваивается определенный атрибут безопасности, который определяет уровень его допуска. Он равен максимальному из атрибутов безопасности объектов, к которому субъект будет иметь доступ.

Если субъект  $U_i \in U$  имеет атрибут  $A_i$ , то он будет иметь доступ ко всем объектам, у которых уровень секретности (атрибут безопасности) будет меньше, либо равен  $A_i$ .

При реализации мандатной модели политики безопасности, как правило, существует два вектора

1. Вектор  $OV = (ov_1, \dots, ov_n)$ , задающий уровни конфиденциальности для всех объектов компьютерной системы ( $n$  – количество объектов).
2. Вектор  $UV = (uv_1, \dots, uv_m)$ , задающий уровни допуска для всех субъектов в компьютерной системе ( $m$  – число субъектов).

Модуль защиты при осуществлении доступа субъекта к объекту сравнивает уровень допуска субъекта с уровнем конфиденциальности объекта и по результатам сравнения разрешает либо запрещает данный доступ. Доступ разрешается, если уровень допуска субъекта больше либо равен уровню конфиденциальности объекта. В ином случае, доступ запрещается.

### **Задание на лабораторную работу**

Пусть задано множество атрибутов безопасности  $A = \{\text{«Совершенно секретно»}, \text{«Секретно»}, \text{«Открытые данные»}\}$ .

1. Получить информацию о количестве объектов и субъектов компьютерной системы из таблицы 1, соответственно Вашему варианту.

2. Реализовать программный модуль, создающий мандатную модель политики безопасности. Реализация данного модуля подразумевает следующее:

2.1. Выбрать идентификаторы пользователей-субъектов, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей-субъектов задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {Ivan, Sergey, Boris}.

2.2. Заполнить вектор  $OV$ , задающий уровни конфиденциальности объектов, случайным образом. Множество атрибутов безопасности  $A$  представлено выше.

2.3. Заполнить вектор  $UV$ , задающий уровни допуска пользователей, случайным образом. Множество атрибутов безопасности  $A$  представлено выше.

2.4. Распечатать на экране вектора  $OV$  и  $UV$ , определяющие уровни конфиденциальности объектов и уровни допуска пользователей. Вывод можно осуществить, например, следующим образом:

Уровни конфиденциальности объектов ( $OV$ ):

Объект\_1: Открытые данные

Объект\_2: Секретно

Объект\_3: Совершенно секретно

Объект\_4: Открытые данные

Уровни допуска пользователей ( $UV$ )

Ivan: Совершенно секретно

Sergey: Секретно

Boris: Открытые данные

3. Реализовать программный модуль, демонстрирующий работу системы в мандатной модели политики безопасности. Данный модуль должен выполнять следующие функции:

3.1. Выполнять идентификацию пользователя при входе в систему. При успешной идентификации пользователя должен осуществляться вход в систему. При неуспешной – выводиться соответствующее сообщение.

3.2. При входе в систему после успешной идентификации пользователя, на экране должен распечатываться список тех объектов системы, к которым у вошедшего пользователя есть доступ. Вывод можно осуществить, например, следующим образом:

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень доступных объектов: Объект\_1, Объект\_4.

Жду ваших указаний >

3.3. После вывода на экран перечня доступных объектов, программа должна ждать указаний пользователя на осуществление действий над объектами в компьютерной системе (команда request). После получения команды request от пользователя, на экран должно выводиться сообщение об успешности либо не успешности операции. Должна поддерживаться операция выхода из системы (quit), после которой должен запрашиваться другой идентификатор пользователя. Диалог можно организовать, например, следующим образом:

Жду ваших указаний > request  
 К какому объекту хотите осуществить доступ? 1  
 Операция прошла успешно  
 Жду ваших указаний > request  
 К какому объекту хотите осуществить доступ? 2  
 Отказ в выполнении операции. Недостаточно прав.  
 Жду ваших указаний > quit  
 Работа пользователя Boris завершена. До свидания.  
 User:

4.Прогнать реализованную программу, продемонстрировав реализованную модель мандатной политики безопасности преподавателю.

5. Оформить в тетради отчет по лабораторной работе согласно примеру, приведенному на последней странице.

### ЗАМЕЧАНИЕ

1. Атрибуты безопасности объектов и уровни доступа субъектов могут быть закодированы цифрами для удобства хранения и сравнения.

Таблица 1

Вариант	Количество субъектов доступа	Количество объектов доступа
1	3	3
2	4	4
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6
11	5	3
12	6	4
13	7	4
14	8	5
15	9	6
16	10	3
17	3	4
18	4	4
19	5	5
20	6	6
21	7	3
22	8	4
23	9	4
24	10	5
25	3	6
26	4	3
27	5	4
28	6	4
29	6	5
30	8	6

### Контрольные вопросы

1. В чем заключается модель мандатной политики безопасности в компьютерной системе?
2. Перечислить группу аксиом, определяющих мандатную модель политики безопасности.
3. Какой уровень допуска должен иметь администратор компьютерной системы?

**Пример оформления отчета по лабораторной работе**

ЛАБОРАТОРНАЯ РАБОТА №

НАЗВАНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

ВЫПОЛНИЛ: ст. гр. .... ФИО

ВАРИАНТ № ...

ЦЕЛЬ ЛАБОРАТОРНОЙ РАБОТЫ

КОЛИЧЕСТВО СУБЪЕКТОВ ДОСТУПА = .....

КОЛИЧЕСТВО ОБЪЕКТОВ ДОСТУПА = .....

ТЕКСТ ПРОГРАММЫ

.....

ПРОГОНКА ПРОГРАММЫ

УРОВНИ КОНФИДЕНЦИАЛЬНОСТИ И ОБЪЕКТОВ \_\_\_\_\_

УРОВНИ ДОПУСКА СУБЪЕКТОВ \_\_\_\_\_

1. Пользователь\_1

Список доступных объектов для пользователя\_1 .....

2. Пользователь\_2

Список доступных объектов для пользователя\_2 .....

3. Пользователь\_3

Список доступных объектов для пользователя\_3 .....

4. Пользователь\_4

Список доступных объектов для пользователя\_4 .....

.....

## ПРИМЕР РАБОТЫ С ПРОГРАММНОЙ МОДЕЛЬЮ МАНДАТНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ

Уровни конфиденциальности объектов (*OV*):

Объект\_1: Открытые данные

Объект\_2: Секретно

Объект\_3: Совершенно секретно

Объект\_4: Открытые данные

Уровни допуска пользователей (*UV*)

Ivan: Совершенно секретно

Sergey: Секретно

Boris: Открытые данные

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень доступных объектов: Объект\_1, Объект\_4.

Жду ваших указаний > request

К какому объекту хотите осуществить доступ? 1

Операция прошла успешно

Жду ваших указаний > request

К какому объекту хотите осуществить доступ? 2

Отказ в выполнении операции. Недостаточно прав.

Жду ваших указаний > quit

Работа пользователя Boris завершена. До свидания.

User: