**ЛАБОРАТОРНАЯ РАБОТА №3**

**Реализация дискреционной модели политики безопасности**

**1 Цель работы:** познакомиться с проблемами реализации политик безопасности в компьютерных системах на примере дискреционной модели

**2 Порядок выполнения работы**:

2.1 Выбрать язык программирования.

2.2 Изучить материал в ***Приложении 1.***

2.3 Пусть имеем множество из 3 пользователей-субъектов O={Администратор, Гость, Пользователь\_1} и множество из 4 объектов U={Файл\_1, Файл\_2, CD-RW, Флеш накопитель}.

Пусть множество возможных действий включает следующие: S={Чтение, Запись, Передача прав}. Кроме этого, существует два дополнительных типа операций - «Полные права», «Полный запрет». Действие «Полные права» разрешает выполнение всех из перечисленных 3 действий, «Полный запрет» запрещает выполнение всех из вышеперечисленных действий. Право «Передача прав» позволяет передавать субъекту свои права на объект другому субъекту.

В данном случае, матрица доступа, описывающая дискреционную политику безопасности, может выглядеть, например, следующим образом (Табл.1).

Таблица 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Объект / Субъект** | **Файл\_1** | **Файл\_2** | **CD-RW** | **Флеш-накопитель** |
| **Администратор** | Полные права | Полные права | Полные права | Полные права |
| **Гость** | Запрет | Чтение | Чтение | Запрет |
| **Пользователь\_1** | Чтение, передача прав | Чтение, запись | Полные права | Полный запрет |

Например, Пользователь\_1 имеет права на чтение и запись в Файл\_2.

Пользователь\_1 может передать свое право на чтение из Файла\_1 другому пользователю. Если Пользователь\_1 передает право на чтение к Файлу\_1 пользователю Гость, то у пользователя Гость появляется право чтения из Файла\_1, соответственно модифицируется матрица доступов.

**Получить данные** о количестве пользователей и объектов компьютерной системы из таблицы 2, соответственно Вашему варианту.

**(БПО-16 варианты 1-20, БПОи варианты 20-30).**

Таблица 2

|  |  |  |
| --- | --- | --- |
| Вариант | Количество субъектов доступа (пользователей) | 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 | 7 | 6 |
| 28 | 8 | 3 |
| 29 | 9 | 4 |
| 30 | 10 | 4 |

2.4 Реализовать программный модуль, создающий матрицу доступа пользователей к объектам компьютерной системы. Реализация данного модуля подразумевает следующее:

2.4.1 Выбрать идентификаторы пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {**Ivan, Sergey, Boris**}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами ко всем объектам).

2.4.2 Реализовать программное заполнение матрицы доступа, содержащей количество пользователей и объектов, соответственно Вашему варианту.

Создать и случайным образом заполнить матрицу доступа субъектов к объектам в виде, аналогичном таблице 1. При заполнении матрицы учесть следующее:

Один из пользователей-субъектов должен являться администратором системы. Для него права доступа ко всем объектам системы должны быть выставлены как полные.

Пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав.

**Замечание 1 по реализации**

Для реализации программной модели матрицы доступов можно использовать массив размерности M x N, где M – количество субъектов, N – количество объектов.

Права доступов в ячейках матрицы доступов можно кодировать трехбитными числами от 0 до 7, например, в следующем виде:

|  |  |  |
| --- | --- | --- |
| Бит доступа по чтению | Бит доступа по записи | Бит передачи прав |

Тогда, соответствие множеств типов доступов и соответствующих значений в матрице доступов будет следующее:

|  |  |  |
| --- | --- | --- |
| **Десятичное число** | **Двоичное число** | **Разрешенные типы доступов** |
| 0 | 000 | Полный запрет |
| 1 | 001 | Передача прав |
| 2 | 010 | Запись |
| 3 | 011 | Запись, Передача прав |
| 4 | 100 | Чтение |
| 5 | 101 | Чтение, Передача прав |
| 6 | 110 | Чтение, Запись |
| 7 | 111 | Полный доступ |

2.5 Реализовать программный модуль, демонстрирующий работу в дискреционной модели политики безопасности. Данный модуль должен выполнять следующие функции:

2.5.1 При запуске модуля должен запрашиваться идентификатор пользователя (должна проводиться идентификация пользователя). При успешной идентификации пользователя должен осуществляться вход в систему. При неуспешной – выводиться соответствующее сообщение.

2.5.2 При входе в систему после успешной идентификации пользователя, на экране должен распечатываться список всех объектов системы с указанием перечня всех доступных прав доступа идентифицированного пользователя к данным объектам. Вывод можно осуществить, например, следующим образом:

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Чтение

Объект2: Запрет

Объект3: Чтение, Запись

Объект4: Полные права

Жду ваших указаний >

2.5.3 После вывода на экран перечня прав доступа пользователя к объектам компьютерной системы, программа должна ждать указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя, на экран должно выводиться сообщение об успешности либо не успешности операции. При выполнении операции передачи прав (grant), должна модифицироваться матрица доступов. Должна поддерживаться операция выхода из системы (quit), после которой должен запрашиваться другой идентификатор пользователя. Диалог можно организовать, например, следующим образом:

Жду ваших указаний > read

Над каким объектом производится операция? 1

Операция прошла успешно

Жду ваших указаний > write

Над каким объектом производится операция? 2

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 3

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 4

Какое право передается? read

Какому пользователю передается право? Ivan

Операция прошла успешно

Жду ваших указаний > quit

Работа пользователя Boris завершена. До свидания.

User:

**Замечание 2 по реализации**

Для контроля возможности заданного типа доступа в рамках предложенной выше программной модели необходимо проверить равенство единице соответствующего бита числа в ячейке матрицы доступов. Для этого можно воспользоваться свойствами операций целочисленного деления я взятия остатка от деления на 2.

Для того, чтобы проверить равенство n-го бита некоторого числа на равенство единице необходимо целочисленно поделить это число на 2n-1 и проверить на нечетность получившееся число. Если после деления получили нечетное число, то n-ый бит исходного числа равен единице, иначе – равен нулю.

**Пример**

Проверить возможность доступа по записи **Пользователя**\_2 к **Файлу\_3.**

1.Берем элемент матрицы доступов, находящийся на пересечении второй строки и третьего столбца. Пусть этот элемент равен 3.

2.Для контроля возможности доступа по чтению, необходимо проверить равенство второго бита числа на единицу. Для этого целочисленно поделим число 3 на 22-1=2.

3.  - число нечетное, то есть второй бит числа 3 равен единице, то есть доступ по записи Пользователя\_2 к Файлу\_3 разрешен.

2.6 Протестировать программу, продемонстрировав реализованную модель дискреционной политики безопасности преподавателю.

**3 Ответьте на контрольные вопросы**:

3.1 Что понимается под политикой безопасности в компьютерной системе?

3.2 В чем заключается модель дискреционной политики безопасности в компьютерной системе?

3.3 Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?

3.4 Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту компьютерной системы?

# **4 Содержание отчета:**

4.1 Задание к лабораторной работе.

4.2 Постановка задачи Вашего варианта.

**Приложение 1**

Под политикой безопасности понимают набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.

При выборе и реализации политики безопасности в компьютерной системе, как правило, работают следующие шаги:

1. В информационную структуру вносится структура ценностей (определяется ценность информации) и проводится анализ угроз и рисков для информации и информационного обмена.
2. Определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей.

Реализация политики безопасности должна быть четко продумана. Результатом ошибочного или бездумного определения правил политики безопасности, как правило, является разрушение ценности информации без нарушения политики.

Существует ряд моделей политик безопасности, отличающихся по возможностям защиты, по качеству защиты, по особенностям реализации. Одной из самых простых и распространенных моделей политик безопасности является дискреционная политика.

# **Дискреционная политика безопасности**

Пусть *О* – множество объектов, *U* – множество пользователей. *S* – множество действий пользователей над объектами. Дискреционная политика определяет отображение  (объектов на пользователей-субъектов). В соответствии с данным отображением, каждый объект  объявляется собственностью соответствующего пользователя , который может выполнять над ними определенную совокупность действий , в которую могут входить несколько элементарных действий (чтение, запись, модификация и т.д.). Пользователь, являющийся собственником объекта, иногда имеет право передавать часть или все права другим пользователям (обладание администраторскими правами).

Указанные права доступа пользователей-субъектов к объектам компьютерной системы записываются в виде так называемой МАТРИЦЫ ДОСТУПА. На пересечении i-ой строки и j-ого столбца данной матрицы располагается элемент Sij – множество разрешенных действий j-ого пользователя над i-ым объектом.

## Пример

### Пусть имеем множество из 3 пользователей {*Администратор, Гость, Пользователь\_1}* и множество из 4 объектов *{Файл\_1, Файл\_2, CD-RW, Флеш-накопитель*}. Множество возможных действий включает следующие: {Чтение, Запись, Передача прав другому пользователю}. Действие «Полные права» разрешает выполнение всех перечисленных 3 действий, Действие «Полный запрет» запрещает выполнение всех из вышеперечисленных действий. В данном случае, матрица доступа, описывающая дискреционную политику безопасности, может выглядеть следующим образом.

Таблица 4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Объект / Субъект | Файл\_1 | Файл\_2 | CD-RW | Флеш-накопитель |
| 1 (Администратор) | Полные права | Полные права | Полные права | Полные права |
| 2 (Гость) | Запрет | Чтение | Чтение | Запрет |
| 3 (Пользователь\_1) | Чтение, передача прав | Чтение, запись | Полные права | Полный запрет |

Например, Пользователь\_1 имеет права на чтение и запись в Файл\_2. Передавать же свои права другому пользователю он не может.

Пользователь, обладающий правами передачи своих прав доступа к объекту другому пользователю, может сделать это. При этом, пользователь, передающий права, может указать непосредственно, какие из своих прав он передает другому.

Например, если Пользователь\_1 передает право доступа к Файлу\_1 на чтение пользователю Гость, то у пользователя Гость появляется право чтения из Файла\_1.

**Приложение 1**

Под политикой безопасности понимают набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.

При выборе и реализации политики безопасности в компьютерной системе, как правило, работают следующие шаги:

1. В информационную структуру вносится структура ценностей (определяется ценность информации) и проводится анализ угроз и рисков для информации и информационного обмена.
2. Определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей.

Реализация политики безопасности должна быть четко продумана. Результатом ошибочного или бездумного определения правил политики безопасности, как правило, является разрушение ценности информации без нарушения политики.

Существует ряд моделей политик безопасности, отличающихся по возможностям защиты, по качеству защиты, по особенностям реализации. Одной из самых простых и распространенных моделей политик безопасности является дискреционная политика.

# **Дискреционная политика безопасности**

Пусть *О* – множество объектов, *U* – множество пользователей. *S* – множество действий пользователей над объектами. Дискреционная политика определяет отображение  (объектов на пользователей-субъектов). В соответствии с данным отображением, каждый объект  объявляется собственностью соответствующего пользователя , который может выполнять над ними определенную совокупность действий , в которую могут входить несколько элементарных действий (чтение, запись, модификация и т.д.). Пользователь, являющийся собственником объекта, иногда имеет право передавать часть или все права другим пользователям (обладание администраторскими правами).

Указанные права доступа пользователей-субъектов к объектам компьютерной системы записываются в виде так называемой МАТРИЦЫ ДОСТУПА. На пересечении i-ой строки и j-ого столбца данной матрицы располагается элемент Sij – множество разрешенных действий j-ого пользователя над i-ым объектом.

## Пример

### Пусть имеем множество из 3 пользователей {*Администратор, Гость, Пользователь\_1}* и множество из 4 объектов *{Файл\_1, Файл\_2, CD-RW, Флеш-накопитель*}. Множество возможных действий включает следующие: {Чтение, Запись, Передача прав другому пользователю}. Действие «Полные права» разрешает выполнение всех перечисленных 3 действий, Действие «Полный запрет» запрещает выполнение всех из вышеперечисленных действий. В данном случае, матрица доступа, описывающая дискреционную политику безопасности, может выглядеть следующим образом.

Таблица 4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Объект / Субъект | Файл\_1 | Файл\_2 | CD-RW | Флеш-накопитель |
| 1 (Администратор) | Полные права | Полные права | Полные права | Полные права |
| 2 (Гость) | Запрет | Чтение | Чтение | Запрет |
| 3 (Пользователь\_1) | Чтение, передача прав | Чтение, запись | Полные права | Полный запрет |

Например, Пользователь\_1 имеет права на чтение и запись в Файл\_2. Передавать же свои права другому пользователю он не может.

Пользователь, обладающий правами передачи своих прав доступа к объекту другому пользователю, может сделать это. При этом, пользователь, передающий права, может указать непосредственно, какие из своих прав он передает другому.

Например, если Пользователь\_1 передает право доступа к Файлу\_1 на чтение пользователю Гость, то у пользователя Гость появляется право чтения из Файла\_1.