ВОРОНЕЖСКИЙ ИНСТИТУТ ВЫСОКИХ ТЕХНОЛОГИЙ – АНОО ВПО

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ЛАБОРАТОРНЫХ РАБОТ

По дисциплине «Защита информации»

Лабораторная работа № 3

«РЕАЛИЗАЦИЯ ДИСКРЕЦИОННОЙ МОДЕЛИ ПОЛИТИКИ БЕЗОПАСНОСТИ»

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

Теоретический материал

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 O – множество объектов, U – множество пользователей. S – множество действий пользователей над объектами. Дискреционная политика определяет отображение $O \to U$ (объектов на пользователей-субъектов). В соответствии с данным отображением, каждый объект $O_j \in O$ объявляется собственностью соответствующего пользователя $U_k \in U$, который может выполнять над ними определенную совокупность действий $S_i \subset S$, 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 S_{ij} – 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, Дисковод}. 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 1

Объект / Субъект	Файл_1	Файл_2	CD-RW	Дисковод
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.

Задание на лабораторную работу

Пусть множество S возможных операций над объектами компьютерной системы задано следующим образом: S={«Доступ на чтение», «Доступ на запись», «Передача прав»}.

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

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

2.1. 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).

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

2.2.1. При заполнении матрицы доступа необходимо учесть, что один из пользователей должен являться администратором системы (допустим, пользователь Ivan). Для него права доступа ко всем объектам должны быть выставлены как полные.

2.2.2. Права остальных пользователей для доступа к объектам компьютерной системы должны заполняться случайным образом с помощью датчика случайных чисел. При заполнении матрицы доступа необходимо учесть, что пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав.

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

3.1. 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.

3.2. 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 >

3.3. 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:

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

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

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	5	4
28	6	4
29	6	5
30	8	6

Контрольные вопросы

1. Что понимается под политикой безопасности в компьютерной системе?
2. В чем заключается модель дискреционной политики безопасности в компьютерной системе?
3. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
4. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту 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

……..

МАТРИЦА ДОСТУПА СУБЪЕКТОВ К ОБЪЕКТАМ В ВИДЕ, АНАЛОГИЧНОМ ПРЕДСТАВЛЕННОМУ В ТАБЛИЦЕ 1

……

ПРИМЕР ПРОГОНКИ ПРОГРАММЫ

User: Sergey

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Полные права

Объект2: Полные права

Объект3: Полные права

Объект4: Полные права

Жду ваших указаний > quit

Работа пользователя Sergey завершена. До свидания.

User: Ivan

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Запрет

Объект2: Запрет

Объект3: Запрет

Объект4: Запрет

Жду ваших указаний > quit

Работа пользователя Ivan завершена. До свидания.

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 > 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:Ivan

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Запрет

Объект2: Запрет

Объект3: Запрет

Объект4: Чтение

Жду ваших указаний > quit

Работа пользователя Ivan завершена. До свидания.

User: