Лабораторная работа № 1.

«Разграничение прав доступа»

Цель работы: изучить методы разграничения доступа пользователей и процессов к ресурсам защищенной информационной системы.

1. Краткие теоретические сведения.

После идентификации и аутентификации пользователя система защиты должна определить его полномочия для последующего контроля санкционированного использования объектов информационной системы.

Процесс определения полномочий пользователей и контроля правомерности их доступа к компьютерным ресурсам называют разграничением доступа, а подсистему защиты, выполняющую эти функции - подсистемой разграничения доступа пользователей к ресурсам компьютерной сети.

Эффективной может быть только та политика разграничения доступа, в основу которой положен принцип - «запрещено все, что не разрешено», а не «разрешено все, что не запрещено».

Если при попытке доступа пользователя к ресурсам компьютерной подсистема разграничения определяет факт несоответствия запроса на доступ пользовательским полномочиям, то доступ блокируется, и могут предусматриваться следующие санкции за попытку несанкционированного доступа:

- предупреждение пользователя;
- отключение пользователя от вычислительной системы на некоторое время;
- полное отключение пользователя от системы до проведения административной проверки;
- подача сигнала службе безопасности о попытке несанкционированного доступа с отключением пользователя от системы.

Существуют следующие методы разграничения доступа:

Разграничение доступа по спискам.

Суть метода состоит в задании соответствий: для каждого пользователя задается список ресурсов и права доступа к ним или для каждого ресурса определяется список пользователей и права доступа к этим ресурсам. С

помощью списков возможно установление прав с точностью до каждого пользователя. Возможен вариант добавления прав или явного запрета доступа. Метод доступа по спискам используется в подсистемах безопасности операционных систем и систем управления базами данных.

Пример списка доступа для определенного ресурса представлен в таблице 1.

Таблица 1. Список доступа для ресурса.

Пользователь 1	Изменение
Пользователь 2	Полный доступ
Пользователь 3	Чтение и выполнение
…	…
Пользователь N	Чтение Изменение Запись

Использование матрицы установления полномочий.

При использовании матрицы установления полномочий применяется матрица доступа (таблица полномочий). В матрице доступа в строках записываются идентификаторы субъектов, которые имеют доступ в компьютерную систему, а в столбцах – объекты (ресурсы) компьютерной системы. В каждой ячейке матрицы может содержаться имя и размер ресурса, право доступа (чтение, запись и др.), ссылка на другую информационную структуру, которая уточняет права доступа, ссылка на программу, которая управляет правами доступа и др. Данный метод является достаточно удобным, так как вся информация о полномочиях сохраняется в единой таблице. Недостаток матрицы – ее возможная громоздкость.
Пример матрицы полномочий представлен в таблице 2.

Таблица 2. Матрица полномочий

	Ресурс 1	Ресурс 2	Ресурс 3	…	Ресурс N
Пользователь 1	00	01	01	…	11
Пользователь 2	01	01	10	…	10
Пользователь 3	00	10	11	…	11
…	…	…	…	…	…
Пользователь N	10	01	00	…	00

В данном примере права доступа задаются двоичным кодом:
00 – нет доступа
01 – только чтение

10 – только запись
11 – полный доступ

Разграничение доступа по уровням секретности и категориям.

Разграничение доступа по уровням секретности и категориям заключается в разделении ресурсов информационной системы по уровням секретности и категориям.

При разграничении по уровню секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем ему определен, например, пользователь имеющий доступ к данным «секретно» также имеет доступ к данным «конфиденциально» и «общий доступ».

При разграничении по категориям задается и контролируется ранг категории пользователей. Соответственно, все ресурсы информационной системы разделяются по уровням важности, причем определенному уровню соответствует категория пользователей. Применение категорий пользователей позволяет упростить процедуры назначения прав пользователей за счет применения групповых политик безопасности.

Пример разграничения доступа по уровням секретности представлен в таблицах 3 и 4.

Таблица 3. Разделение ресурсов по уровням секретности.

Уровень секретности	Ресурс
Общий доступ	Ресурс 3, Ресурс 5
Конфиденциально	Ресурс 4
Секретно	Ресурс 1, Ресурс 6, Ресурс 7
Совершенно секретно	Ресурс 2, Ресурс 8

Таблица 4. Разделение пользователей по уровням секретности.

Уровень секретности	Пользователь
Общий доступ	Пользователь 4
Конфиденциально	Пользователь 1, Пользователь 3
Секретно	Пользователь 5, Пользователь 2
Совершенно секретно	Пользователь 6

Таблица 5. Матрица доступа на основе разделения по уровням секретности

	Ресурс 1	Ресурс 2	Ресурс 3	Ресурс 4	Ресурс 5	Ресурс 6	Ресурс 7	Ресурс 8

Пользователь 1	-	-	+	+	+	-	-	-
Пользователь 2	+	-	+	+	+	+	+	-
Пользователь 3	-	-	+	+	+	-	-	-
Пользователь 4	-	-	+	-	+	-	-	-
Пользователь 5	+	-	+	+	+	+	+	-
Пользователь 6	+	+	+	+	+	+	+	+

Парольное разграничение доступа.

Парольное разграничение, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

2. Порядок выполнения лабораторной работы.

1. Разработать модель предприятия с указанием организационной структуры (сотрудники, отделы) и информационных ресурсов.

2. Привести список доступа к одному из ресурсов.

3. Привести матрицу доступа для всех пользователей и ресурсов.

4. Присвоить всем ресурсам и пользователям уровни секретности. На основе распределения составить общую таблицу доступа к ресурсам.

3. Контрольные вопросы.

1. Что означает термин «разграничение доступа»?

2. Приведите основные методы разграничения доступа.

3. В чем заключается метод разграничения по списку?

4. Как строится матрица установления полномочий?

5. В чем преимущества и недостатки матриц установления полномочий?

6. В чем заключается разграничение доступа по уровням секретности и категориям?