Практическая работа №5

ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА

Цель работы. Изучить способы разграничения доступа. Научиться распределять права доступа сотрудникам предприятия в зависимости от их должностных обязанностей.

Краткие сведения из теории

Разграничение доступа к элементам защищаемой информации заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности беспрепятственного доступа к информации в пределах его полномочий и исключить возможности превышения своих полномочий. В этих целях разработаны и реализованы на практике методы и средства разграничения доступа к устройствам ЭВМ, программам обработки информации, полям (областям ОЗУ, ПЗУ) и массивам (базам) данных. Само разграничение может осуществляться несколькими способами, а именно:

1) списки контроля доступа (ACL – Access Control Lists);

2) избирательное или дискреционное управление доступом (DAC – Discretionary Access Control, матрицей контроля доступа), схема которого представлена на рисунке 1;

3) полномочное (мандатное) управление доступом (MAC – Mandatory Access Control) – по уровням секретности, схема которого представлена на рисунке 2.

Разграничение доступа по *спискам контроля доступа* заключается в том, что для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа. Наиболее полной моделью распределения полномочий является матрица доступа, в строках которой перечислены субъекты, в столбцах – объекты; в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия, текущие права других субъектов) и разрешенные виды доступа. В таблице 1 представлен пример разграничения доступа в структуре университета, права пользователь соответствуют следующим сокращениям: *X* – нет прав; *R* – чтение; *W* – запись; *C* – создание; *E* – редактирование; *D* – удаление.

Избирательное или дискреционное управление доступом (разграничение доступа по матрицам полномочий) предполагает формирование двумерной

матрицы, по строкам которой содержатся идентификаторы зарегистрированных пользователей, а по столбцам – идентификаторы защищаемых элементов данных. Элементы матрицы содержат информацию об уровне полномочий соответствующего пользователя относительно соответствующего элемента. Недостатком метода разграничения доступа на основе матрицы полномочий является то, что с увеличением масштаба данная матрица может оказаться слишком громоздкой. Преодолеть данный недостаток можно путем применения следующих рекомендаций по сжатию матрицы установления полномочий:

– пользователей, имеющих идентичные полномочия, в группы;

– объединение ресурсов, полномочия на доступ к которым совпадают.

Таблица 1 – **Пример таблицы разграничения доступа по списку контроля доступа**

Субъект	Объект			
	персональные данные	финансовые отчеты	учебно-методические комплексы	приказы
Ректорат	*R*	*R*	*R*	*R, W, C, D*
Бухгалтерия	*R*	*W, C, E*	*R*	*R*
Преподаватели	*X*	*X*	*W, R, C, E, D*	*R*
Студенты	*X*	*X*	*R*	*R*

Таблица 2 – **Пример таблицы избирательного разграничения доступа**

Субъект	Объект			
	персональные данные ассистента	финансовый отчет	методическое пособие	приказ
Ректор	*R*	*R*	*R*	*R, W, C, D*
Главный бухгалтер	*R*	*W, C, E*	*R*	*R*
Преподаватель	*X*	*X*	*W, R, C, E, D*	*R*
Студент	*X*	*X*	*R*	*R*

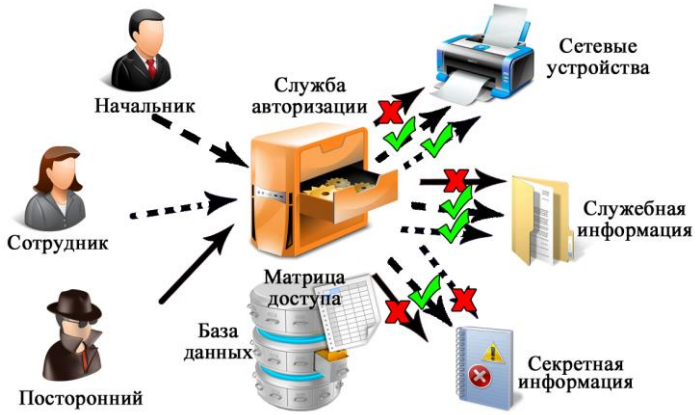

Рисунок 1 – Схема реализации дискреционного управления доступом

Полномочное (мандатное) управление доступом есть способ разового разрешения на допуск к защищаемому элементу данных. Заключается он в том, что каждому защищаемому элементу присваивается персональная уникальная метка, после чего доступ к этому элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владелец элемента.

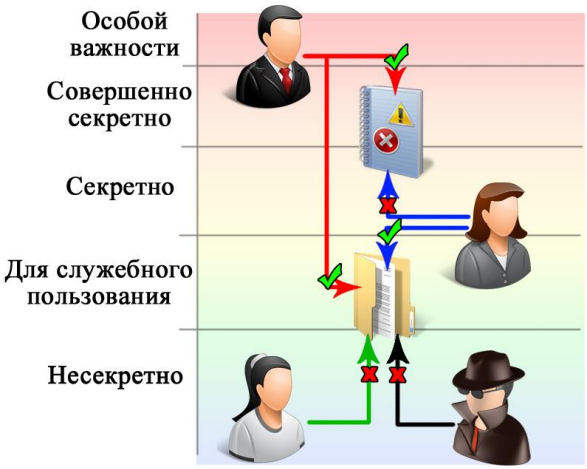

Рисунок 2 – Схема реализации мандатного управления доступом

Полномочное (мандатное) управление доступом заключается в том, что защищаемые данные распределяются по массивам (базам) таким образом, чтобы в каждом массиве (каждой базе) содержались данные одного уровня секретности (например, только с грифом «конфиденциально» или только «секретно», или только «совершенно секретно», или каким-либо другим). Каждому зарегистрированному пользователю предоставляется вполне определенный уровень допуска (например, «секретно», «совершенно секретно» и т. п.). Тогда пользователю разрешается доступ к массиву (базе) своего уровня и массивам (базам) низших уровней и запрещается доступ к массивам (базам) более высоких уровней.

В таблице 3 представлен пример дискреционного управления доступом на железнодорожной станции, причем символ «+» означает наличие разрешенного действия (строка) для субъекта (столбец). В информационной системе выделены следующие субъекты информационной системы: начальник станции, дежурный по станции, начальник участка СЦБ, старший электромеханик, электромеханик, диспетчер отделения дороги.

Таблица 3 – **Пример дискреционного управления доступом на железнодорожной станции**

Действия субъектов согласно ПРД	Субъекты информационной системы					
	начальник станции	дежурный по станции	начальник участка СЦБ	старший электромеханик	электромеханик	диспетчер отделения дороги
Получение информации о поездной обстановке на станции	+	+	+	+	+	+
Получение специальной технологической информации по станции	+	+	–	–	–	–
Получение диагностической информации о системе ПРЦ по фиксированным запросам	–	–	+	+	+	–
Управление объектами станции с обеспечением условий безопасности движения поездов	+	+	–	–	–	–
Техническое обслуживание объектов управления на станции	–	–	+	+	+	–
Обслуживание технических средств ПРЦ	–	–	+	+	+	–

Порядок выполнения работы

1 Выполнить разграничение доступа по спискам контроля доступа для всех пользователей информационной системы Белорусской железной дороги из практической работы № 1. В таблице 4 разделить всех пользователей на не менее чем 5 групп. В таблице 5 прописать разрешенные действия для групп и активов, для обозначения прав использовать следующие сокращения: *X* – нет прав; *R* – чтение; *W* – запись; *C* – создание; *E* – редактирование; *D* – удаление.

Таблица 4 – **Разделение пользователей на группы**

Группа пользователей	Состав группы пользователей			

Таблица 5 – **Разграничение прав пользователей по спискам контроля доступа**

Актив	Группы пользователей				

2 Выполнить избирательное разграничение доступа для всех пользователей предприятия (не менее семи). Задание выполнить в виде таблицы 6.

Таблица 6 – **Разграничение прав пользователь по избирательному контролю доступа**

Пользователи	Активы					

3 Выполнить полномочное управление доступом для всех пользователей предприятия. В таблицах 7 и 8 распределить метки критичности для пользователей (не менее семи) и активов (не менее семи).

Таблица 7 – **Определение меток критичности для пользователей**

Пользователи	Метка критичности				
	Особой важности	Совершенно секретно	Секретно	Для служебного пользования	Несекретно

Таблица 8 – **Определение меток критичности для активов**

Активы	Метка критичности				
	Особой важности	Совершенно секретно	Секретно	Для служебного пользования	Несекретно

Содержание отчета

1 Цель работы.
2 Результаты выполнения задания.
3 Описание информационного объекта.
4 Таблицы правил разграничения доступа.
5 Вывод по работе.

Контрольные вопросы

1 Основные отличия избирательного и полномочного управления доступом.
2 В каких сферах может использоваться мандатное управление доступом?
3 Достоинства и недостатки мандатного разграничения доступа.
4 Особенности разграничения доступа по спискам.