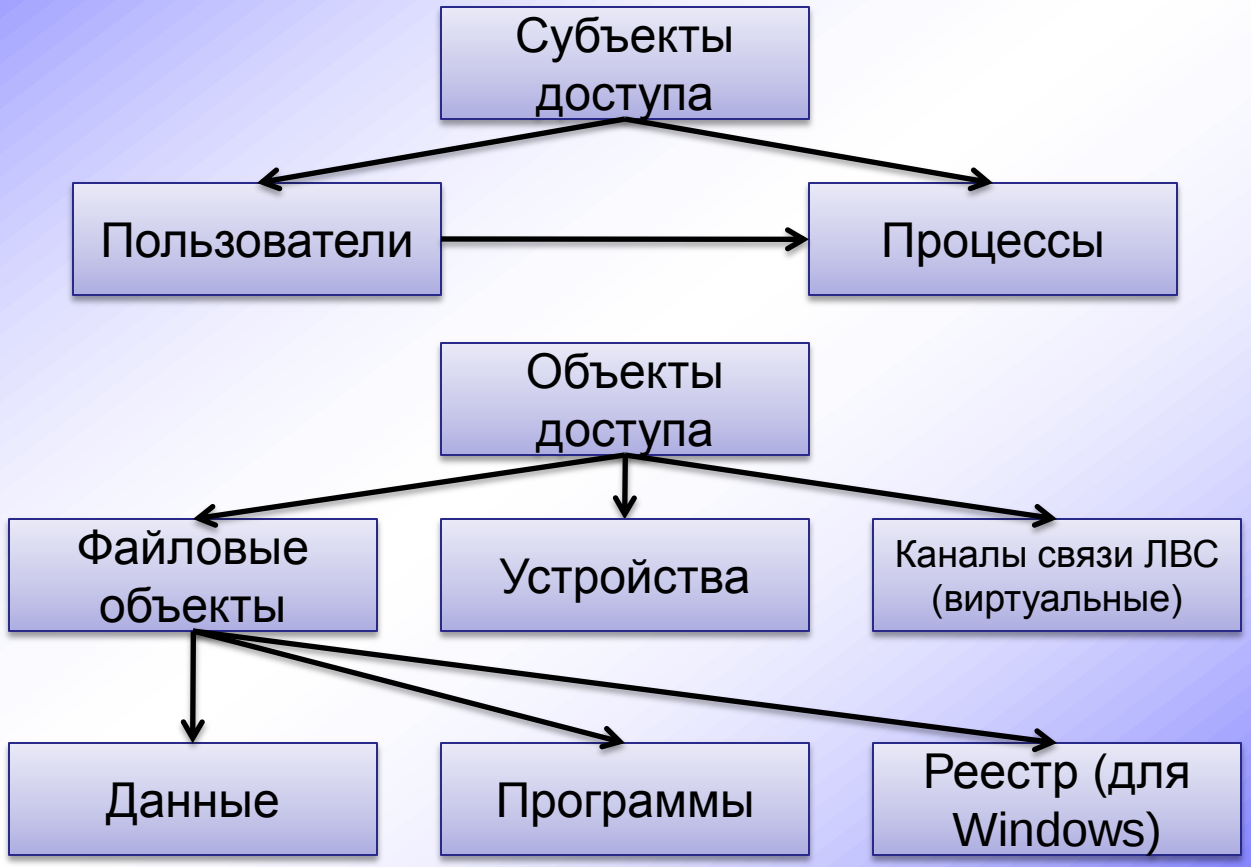
Лекция №5

Управление доступом к ресурсам ОС

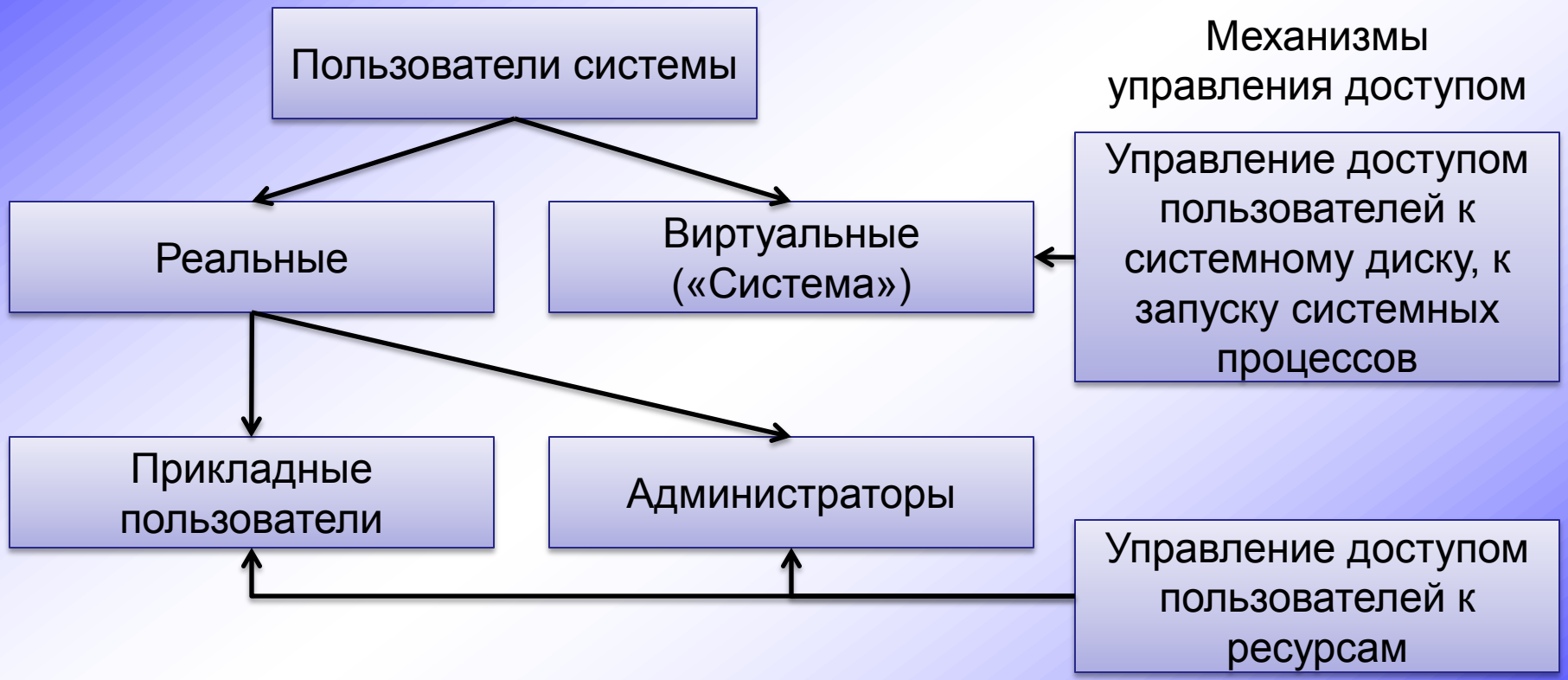
(часть 2)

Классификация субъектов и объектов доступа

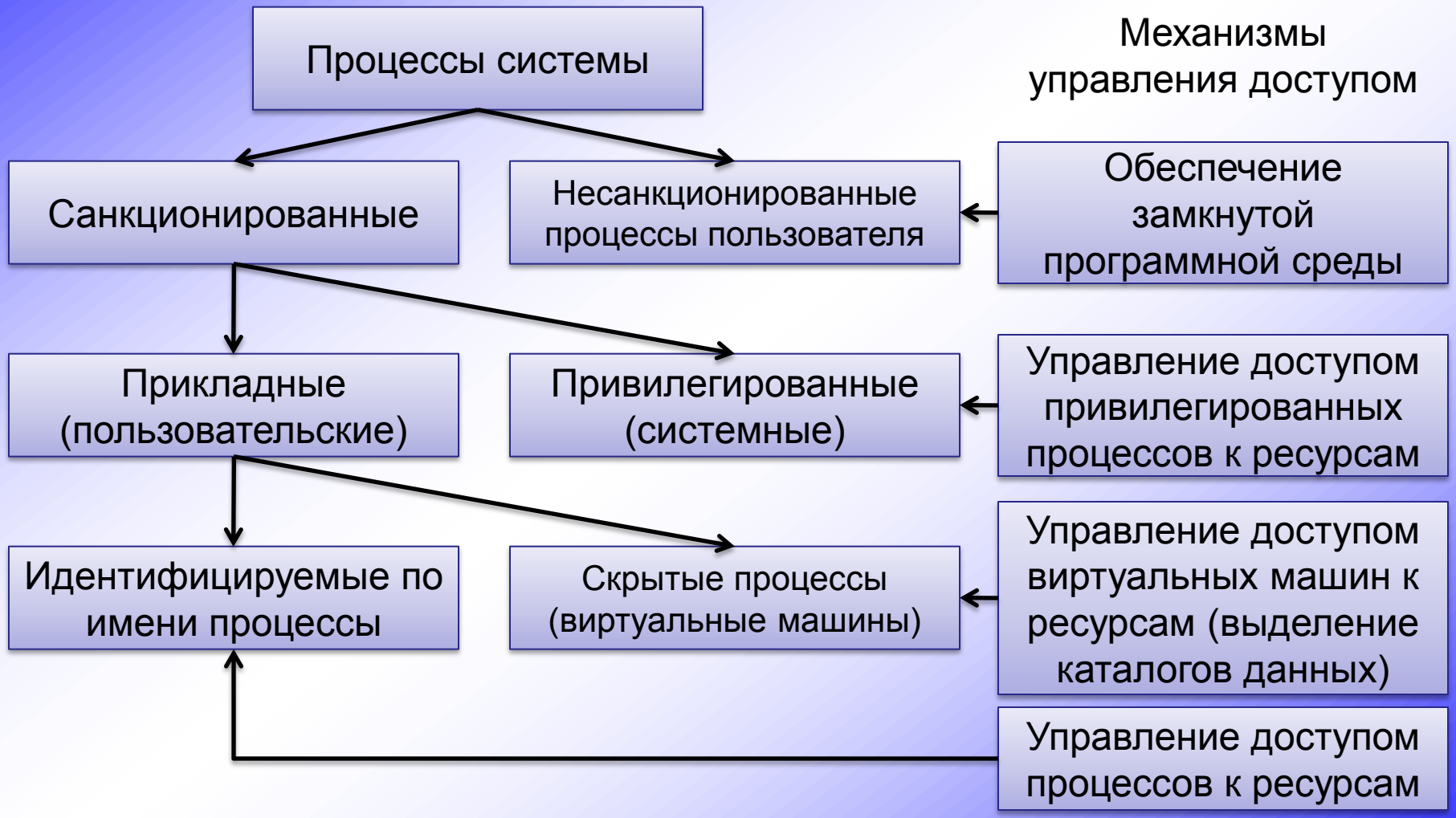
Общая классификация субъектов и объектов доступа



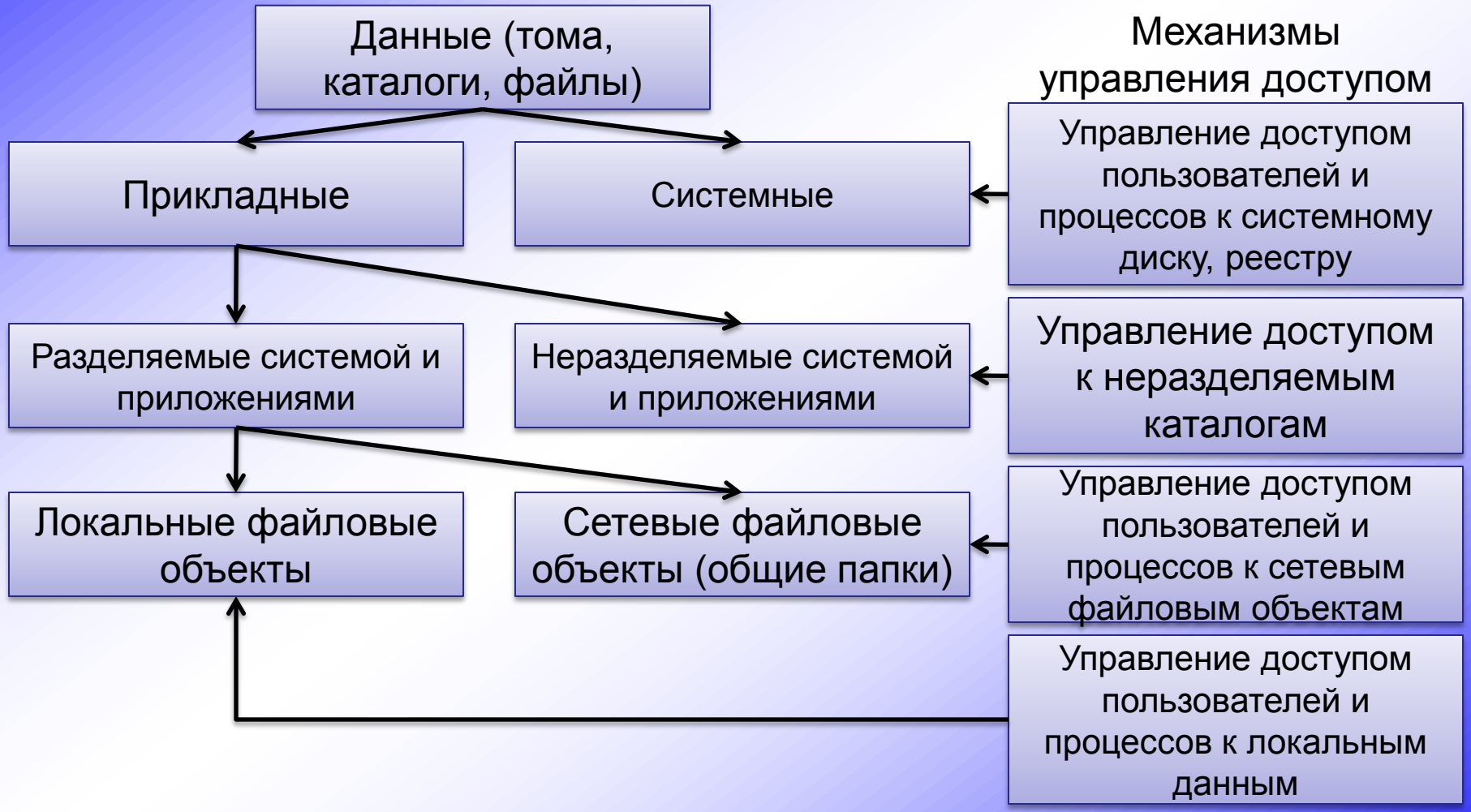
Классификация пользователей



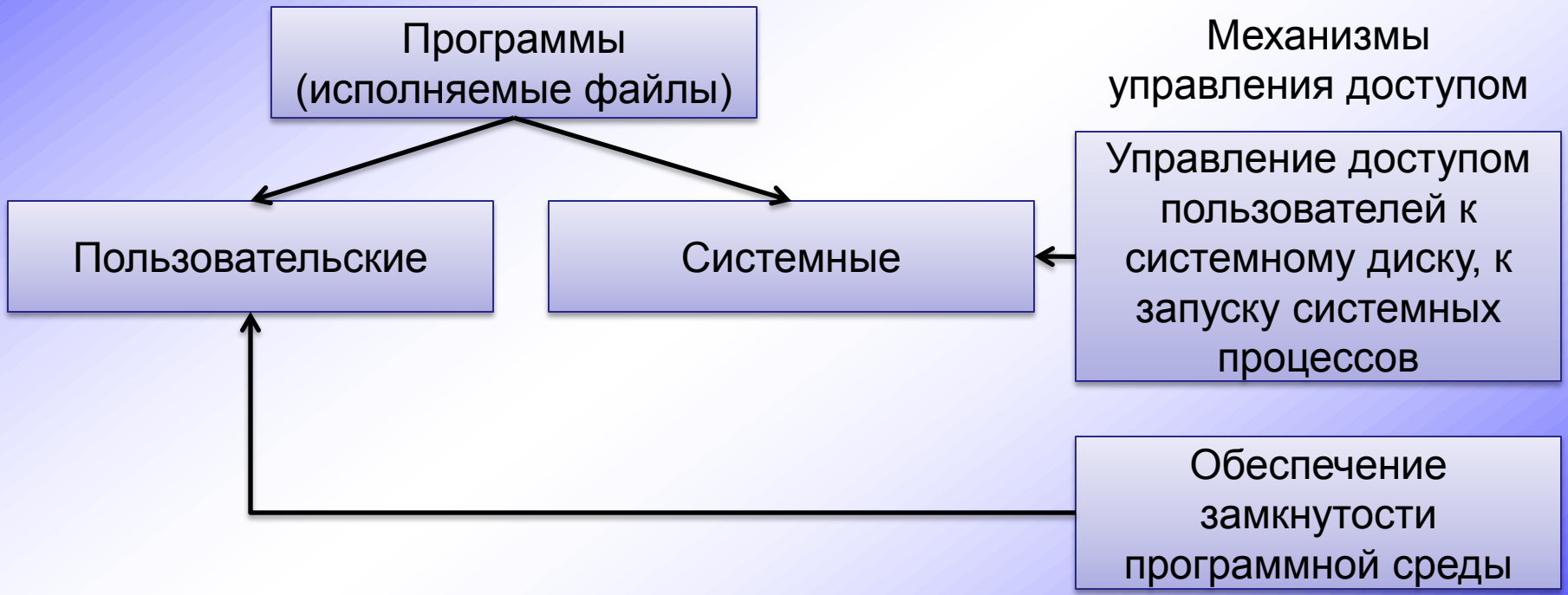
Классификация процессов



Классификация файловых объектов данных



Классификация файловых объектов программ



Классификация устройств

Реализация схемы управления доступом

Дискреционный механизм управления доступом

- Определение – способ обработки запросов диспетчером доступа, основанный на задании правил разграничения доступа в диспетчере непосредственно матрицей доступа.
- Учётная информация субъекта (группы субъектов) и объекта – их идентификаторы (например, имя пользователя и имя файлового объекта).
- Может быть реализована любая модель управления доступом.

Матрица доступа при дискреционном механизме

	C_1	C_2	C_3	…	C_k
O_1	Чт/Зп	Зп	Зп	…	0
O_2	Зп	Чт/Зп	Зп	…	Зп
O_3	Зп	0	Чт/Зп	…	Зп
…	…	…	…	…	…
O_k	Зп	0	Зп	…	Чт/Зп

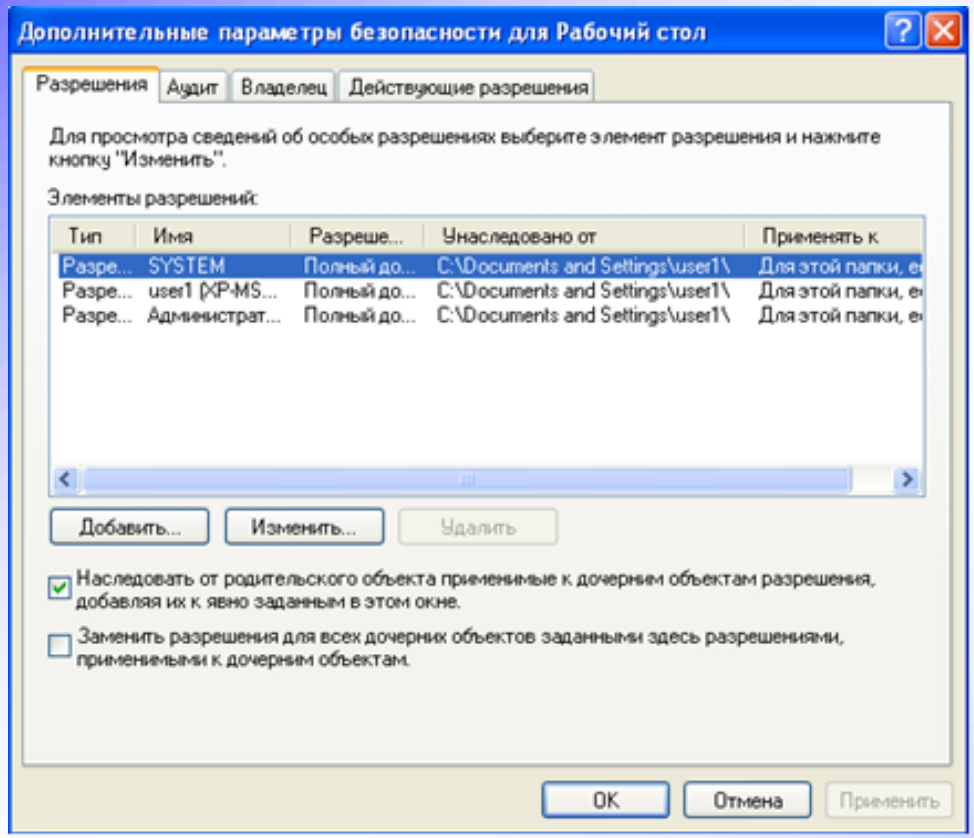
Реализация дискреционного механизма в Windows

Каждому объекту соответствует дескриптор безопасности, включающий:

- флаги, отвечающие за наследование разрешений от родительского объекта;
- идентификатор владельца;
- идентификатор основной группы для объекта;
- список управления доступом (ACL), содержащий списки имеющих право на доступ к объекту (DACL) и список регистрируемых действий (SACL).

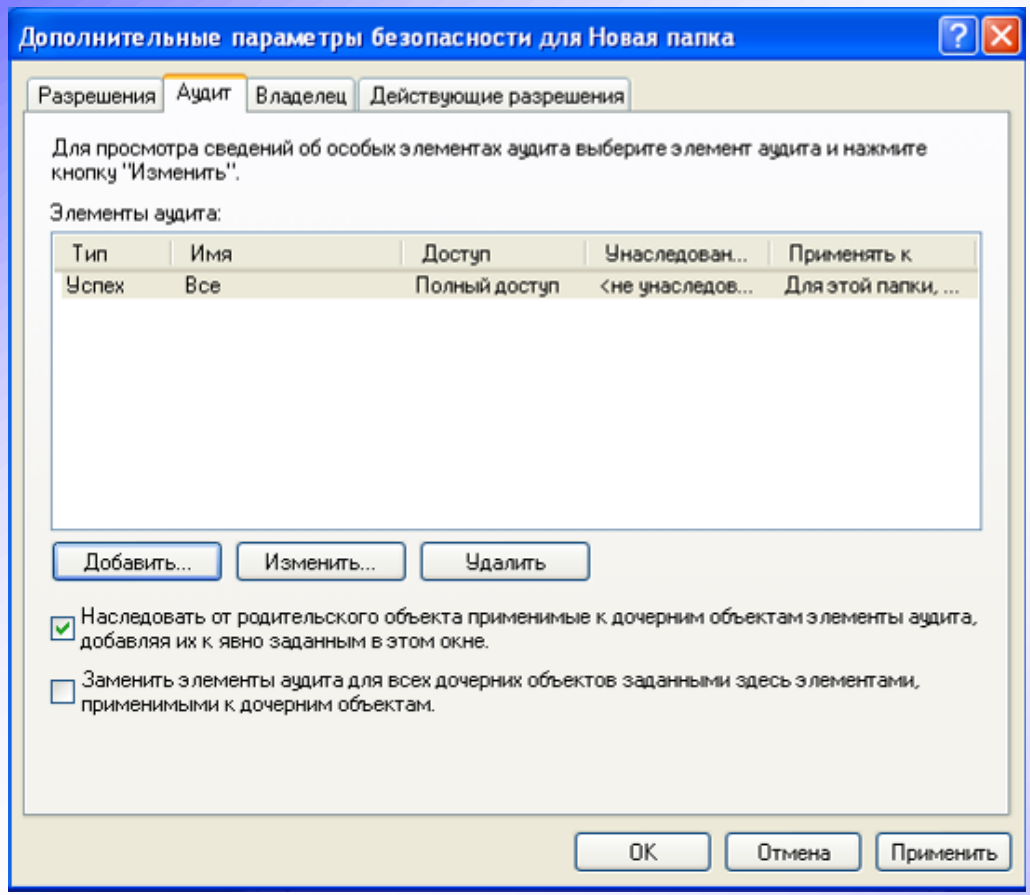
Если отсутствует: DACL, то все имеют полный доступ к объекту; SACL, то события не подвергаются аудиту.

Список управления избирательным доступом (DACL)



Существует для каждого объекта и содержит столбцы матрицы управления доступом, т. е. имена всех пользователей и групп, имеющих доступ к объекту, и их разрешения на доступ.

Системный список управления доступом (SACL)



Существует для каждого объекта и содержит перечень событий, подвергаемых аудиту для данного объекта.

Каноническая модель управления доступом

	C_1	C_2	C_3	…	C_k
O_1	1	0	0	…	0
O_2	0	1	0	…	0
O_3	0	0	1	…	0
…	…	…	…	…	…
O_k	0	0	0	…	1

1, если $i=j$;

иначе 0.

- i – порядковый номер объекта доступа;
- j – порядковый номер субъекта доступа;
- 1 – полный доступ;
- 0 – запрещение доступа.

Каноническая модель управления доступом

- Под канонической моделью управления доступом для линейно упорядоченных множеств субъектов (групп субъектов) и объектов (групп объектов) доступа понимается модель, описываемая матрицей доступа, элементы главной диагонали которой «1» разрешают полный доступ субъектов к объектам, остальные элементы «0» запрещают доступ субъектов к объектам.
- Диспетчер доступа реализует механизм управления доступом корректно только в том случае, если его настройками (заданием учетных записей субъектов и объектов доступа и правил разграничения доступа) можно реализовать каноническую модель управления доступом.

Канал взаимодействия субъектов и объектов

- Каноническая модель управления доступом характеризуется полным разграничением доступа субъектов к объектам, при котором субъекты не имеют каналов взаимодействия – каналов обмена информацией.
- Канал взаимодействия субъектов доступа – реализуемая диспетчером доступа возможность обмена субъектами доступа информацией в рамках канонической модели управления доступом.

Модель управления доступом с взаимодействием субъектов

	C_1	C_2	C_3	…	C_k
O_1	Чт/Зп	Д	Д	…	Д
O_2	Д	Чт/Зп	Д	…	Д
O_3	Д	Д	Чт/Зп	…	Д
…	…	…	…	…	…
O_k	Д	Д	Д	…	Чт/Зп

Чт/Зп, если $i=j$;

иначе Д.

- Чт – доступ с использованием «чтения»;
- Зп – доступ с использованием «записи» (изменение);
- Д – доступ с использованием «добавления».

Методы управления каналами взаимодействия

- Под методом произвольного управления виртуальными каналами взаимодействия субъектов доступа понимается управление по усмотрению субъекта, имеющего полный доступ к информации. При этом решение о предоставлении другому субъекту информации из объекта по виртуальному каналу принимается непосредственно субъектом, имеющим полный доступ к этой информации.
- Под методом принудительного управления каналами взаимодействия субъектов понимается управление, реализуемое не по усмотрению субъекта, а на основании некоторой параметрической шкалы оценки субъектов и объектов доступа.

Полномочное управление доступом

- Множества $C = \{C_1,..., C_k\}$ и $O = \{O_1,..., O_k\}$ – линейно полномочно упорядоченные множества субъектов и объектов доступа. Чем меньше порядковый номер субъекта доступа, тем большими полномочиями по доступу к объектам он обладает. Чем меньше порядковый номер объекта доступа, тем большие полномочия необходимы для доступа к нему.
- При полномочном управлении доступом недопустима передача информации (организация канала взаимодействия субъектов) из объектов с более высокими полномочиями (меньшим номером) доступа к ним в объекты с меньшими полномочиями (большим номером) доступа к ним.

Полномочная модель с произвольным управлением каналами взаимодействия

	C_1	C_2	C_3	…	C_k
O_1	Чт/Зп	Д	Д	…	Д
O_2	0	Чт/Зп	Д	…	Д
O_3	0	0	Чт/Зп	…	Д
…	…	…	…	…	…
O_k	0	0	0	…	Чт/Зп

Чт/Зп, если $i=j$;

0, если $i>j$;

Д, если $i<j$.

Полномочная модель с принудительным управлением каналами взаимодействия

	C_1	C_2	C_3	…	C_k
O_1	Чт/Зп	0	0	…	0
O_2	Чт	Чт/Зп	0	…	0
O_3	Чт	Чт	Чт/Зп	…	0
…	…	…	…	…	…
O_k	Чт	Чт	Чт	…	Чт/Зп

Чт/Зп, если $i=j$;

Чт, если $i>j$;

0, если $i<j$.

Полномочная модель с комбинированным управлением каналами взаимодействия

	C_1	C_2	C_3	…	C_k
O_1	Чт/Зп	Д	Д	…	Д
O_2	Чт	Чт/Зп	Д	…	Д
O_3	Чт	Чт	Чт/Зп	…	Д
…	…	…	…	…	…
O_k	Чт	Чт	Чт	…	Чт/Зп

Чт/Зп, если $i=j$;

Чт, если $i>j$;

Д, если $i<j$.

Присвоение меток безопасности

- Метки безопасности являются элементами линейно упорядоченного множества

  $M = \{M_1,\ldots,M_k\}$ и задаются субъектам и объектам доступа.
- Чем выше полномочия субъекта и объекта (меньше их порядковый номер в линейно полномочно упорядоченных множествах субъектов и объектов – $C = \{C_1,\ldots, C_k\}$ и $O = \{O_1,\ldots, O_k\}$), тем меньшее значение метки безопасности M_i, $i = 1,\ldots,k$ им присваивается, т.е.: $M_1 < M_2 < M_3 < \ldots < M_k$.

Категорирование прав доступа

Метки безопасности могут задаваться:

- по степени секретности, т.е. «открытая», «служебная», «конфиденциальная» и т.д.;
- на основе принципа «начальник-подчинённый», т.е. запрет любого доступа подчинённого к объектам начальника, разрешение доступа на чтение начальнику к объектам подчинённого;
- с учётом наличия системных объектов, т.е. пользователю разрешается только доступ на чтение системных объектов.

Использование неиерархических меток

- При наличии в системе нескольких типов информации (бухгалтерская, персональные данные и т.д.) по числу обрабатываемых типов информации вводятся метки M_i.
- Однотипная метка присваивается типу информации и пользователю (группе пользователей), которые имеют право обработки данной информации.
- Назначение однотипной метки предполагает полный доступ пользователя к информации, несовпадение меток – запрет доступа.

Правила разграничения доступа

- Разграничение доступа диспетчером реализуется на основе правил, определяющих отношение линейного порядка на множестве *M*, где для любой пары элементов из множества *M*, задается один из типов отношения: {>,<,=}.
- M_c — метка безопасности субъекта (группы субъектов) доступа.
- M_o — метка безопасности объекта (группы объектов) доступа.
- Метка безопасности с порядковым номером *i* – M_i устанавливается для субъекта доступа с порядковым номером *i* – C_i и для объекта доступа с порядковым номером *i* – O_i.

Правила разграничения доступа

Полномочная модель управления доступом с произвольным управлением каналами взаимодействия субъектов доступа:

- субъект С имеет доступ к объекту О в режиме «Чтения» в случае, если выполняется условие $M_c = M_o$;
- субъект С имеет доступ к объекту О в режиме «Записи» в случае, если выполняется условие $M_c = M_o$;
- субъект С имеет доступ к объекту О в режиме «Добавления» в случае, если выполняется условие $M_c > M_o$.

Правила разграничения доступа

Полномочная модель управления доступом с принудительным управлением каналами взаимодействия субъектов доступа:

- субъект С имеет доступ к объекту О в режиме «Чтения» в случае, если выполняется условие $M_C <= M_O$;
- субъект С имеет доступ к объекту О в режиме «Записи» в случае, если выполняется условие $M_C = M_O$.

Правила разграничения доступа

Полномочная модель управления доступом с комбинированным управлением каналами взаимодействия субъектов доступа:

- субъект С имеет доступ к объекту О в режиме «Чтения» в случае, если выполняется условие

  $M_C <= M_O$;

- субъект С имеет доступ к объекту О в режиме «Записи» в случае, если выполняется условие

  $M_C = M_O$;

- субъект С имеет доступ к объекту О в режиме «Добавления≫ в случае, если выполняется условие $M_C > M_O$.

Корректность реализации полномочной модели

Мандатный механизм управления доступом позволяет корректно реализовать полномочные модели управления доступом при условии, что всем субъектам и объектам доступа сопоставлены метки безопасности.

Совместное использование дискреционного и мандатного механизмов

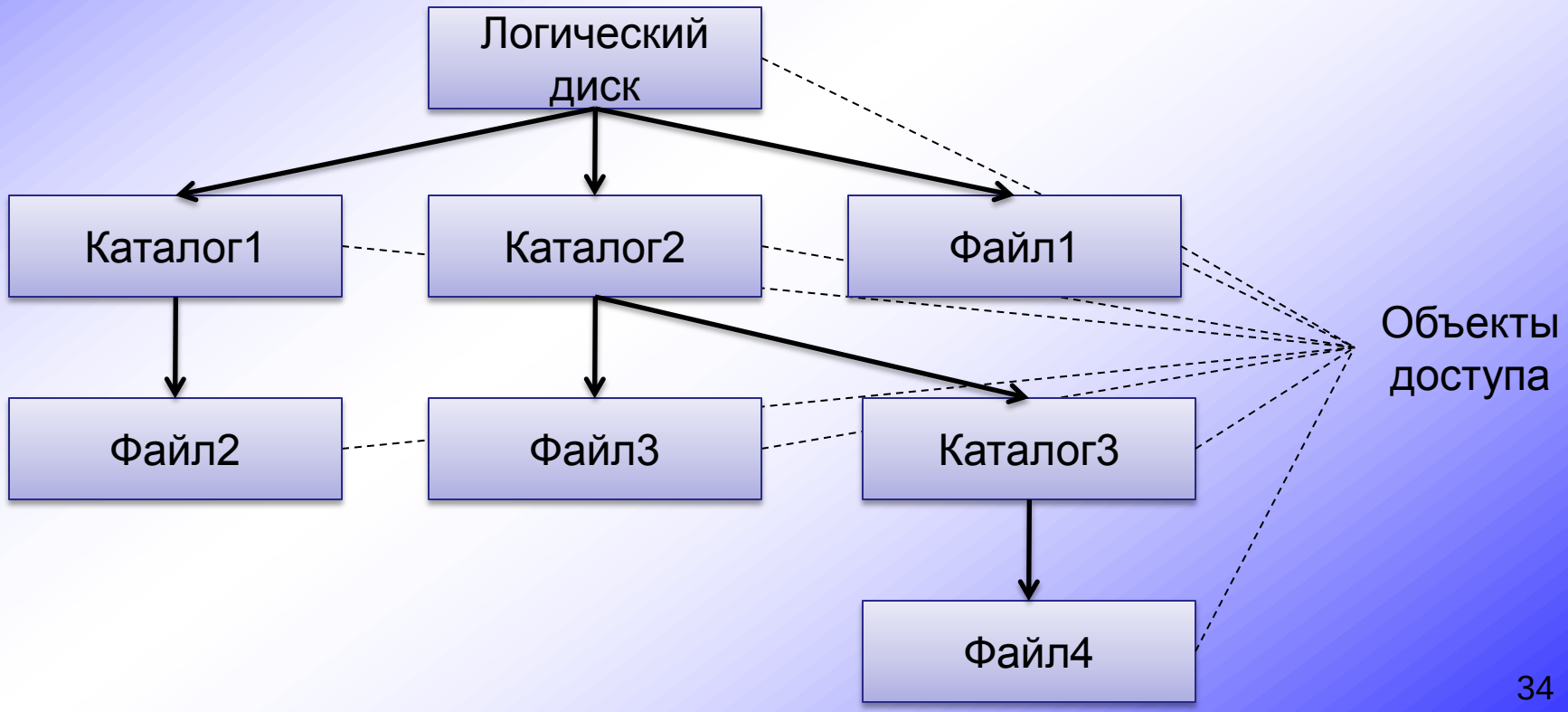
	C_1	C_2	C_3	…	C_k
O_1	Чт/Зп	Д	Д	…	Д
O_2	Чт	Чт/Зп	Д	…	Д
O_3	Чт	Чт	Чт/Зп	…	Д
…	…	…	…	…	…
O_k	0	Чт	Чт	…	Чт/Зп

- Мандатным механизмом реализована каноническая полномочная модель управления доступом с комбинированным управлением каналом взаимодействия.
- Дискреционным механизмом запрещено чтение субъектом C_1 объекта O_k.

Разграничение доступа к иерархическим объектам

Иерархические объекты доступа

Файловая система – иерархическая система, в которой объекты на каждом уровне иерархии (тома, каталоги, файлы) являются объектами доступа.



Задачи разграничения доступа к иерархическим объектам

- Предоставление пользователю возможности доступа к расположенному на нижних уровнях иерархии объекту, к которому ему разрешён доступ.
- Недопущение записи данных пользователем в объекты, расположенные на иерархическом пути к искомому объекту доступа, для исключения несанкционированного обмена информацией.

Метки безопасности для иерархических объектов доступа

Правила назначения меток безопасности.

1. Метки безопасности из множества $M = \{M_1,\ldots,M_k\}$, используемого в полномочной модели управления доступом, присваиваются объектам доступа (без учета их иерархии), к которым следует разграничивать доступ. Процедура назначения меток безопасности начинается с разметки данных объектов.
2. Метки безопасности должны присваиваться всем включающим элементам иерархии, вплоть до элемента, являющегося объектом доступа. Для разметки включающих элементов, не являющихся непосредственно объектами доступа, но к которым следует разграничить доступ, вводится метка M_{k+1}. Причем для элементов множества M должно выполняться условие: $M_1 < M_2 < M_3 < \ldots < M_k < M_{k+1}$.

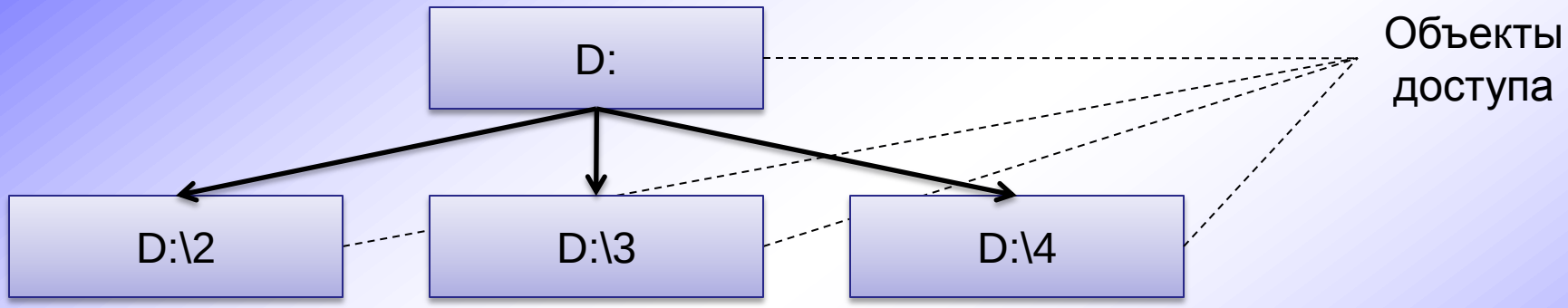
Метки безопасности для иерархических объектов доступа

3. Включаемому элементу может не присваиваться метка безопасности, тогда включаемый элемент наследует метку безопасности (имеет то же значение метки) включающего его элемента.
4. Вводится группа старших (корневых) элементов иерархии O_{k+1}, включающих объекты доступа. Данной группе объектов должна присваиваться метка безопасности M_{k+1}.
5. К группе старших (корневых) элементов иерархии O_{k+1} при сопоставлении ей метки M_{k+1} разрешается доступ по «чтению».

Матрица доступа при наличии иерархических объектов доступа

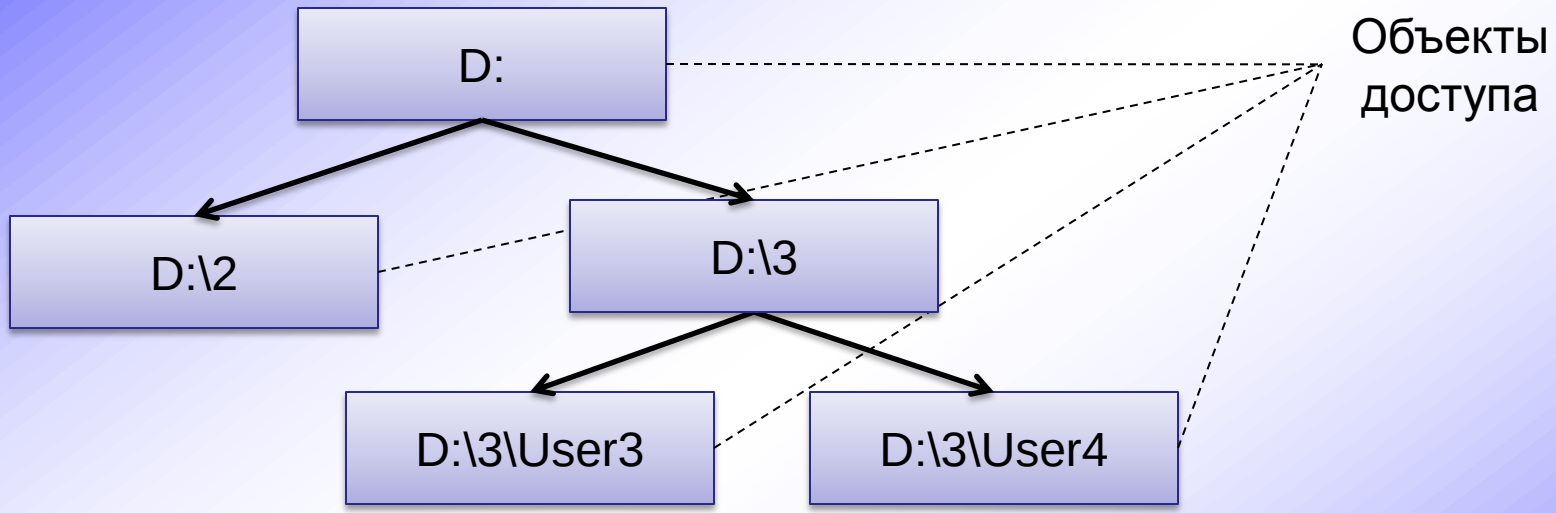
	C_1	C_2	C_3	…	C_k
O_1	Чт/Зп	Д	Д	…	Д
O_2	Чт	Чт/Зп	Д	…	Д
O_3	Чт	Чт	Чт/Зп	…	Д
…	…	…	…	…	…
O_k	Чт	Чт	Чт	…	Чт/Зп
O_{k+1}	Чт	Чт	Чт	…	Чт

Пример назначения меток безопасности для иерархических объектов доступа



Метка безопасности объектов	Объекты доступа	Права доступа субъектов
2	D:\2	2 – Чт/Зп; 3,4 – Д.
3	D:\3	2 – Чт; 3 – Чт/Зп; 4 – Д.
4	D:\4	2,3 – Чт; 4 – Чт/Зп.
5	D:	2,3,4 – Чт.

Пример назначения меток безопасности для иерархических объектов доступа



Метка безопасности объектов	Объекты доступа	Права доступа субъектов
2	D:\2	2 – Чт/Зп; 3,4 – Д.
3	D:\3\User3	2 – Чт; 3 – Чт/Зп; 4 – Д.
4	D:\3\User4	2,3 – Чт; 4 – Чт/Зп.
5	D:	2,3,4 – Чт.

Каталог D:\3 не является объектом доступа, поэтому по умолчанию он наследует метку безопасности включающего объекта, т.е. 5 (D:)

Способы назначения ресурсам меток безопасности

Общий формат определения ресурса устройства (накопителя):

- имя съёмного устройства\каталог\подкаталог\ ...\файл – для доступа к файлу;
- имя съёмного устройства\каталог\подкаталог – для доступа к каталогу (подкаталогу);
- имя съёмного устройства – для доступа ко всему устройству в целом, которое может содержать каталоги и файлы (например, к устройству ввода данных).

Способы назначения ресурсам меток безопасности

- При разметке устройства метка безопасности должна присваиваться собственно устройству. Присвоение устройству метки означает разрешение полного доступа (чтение и запись) к устройству только пользователей с аналогичной меткой. Правила доступа остальных пользователей к устройству определяются реализуемыми каналами взаимодействия субъектов доступа в матрице доступа.
- Разметка накопителя для возможности сохранения на нём объектов. На накопителе санкционированным пользователем создаётся новый каталог, которому присваивается имя и метка безопасности. Доступ на чтение/запись данных в этот каталог будет иметь субъект с такой же меткой безопасности. При работе субъектов с разными метками безопасности для каждого субъекта создаётся свой каталог.

Наследование прав доступа

Реализация механизма наследования прав доступа

При дискреционном управлении доступом набор правил разграничения доступа для каждого объекта иерархии формируется из:

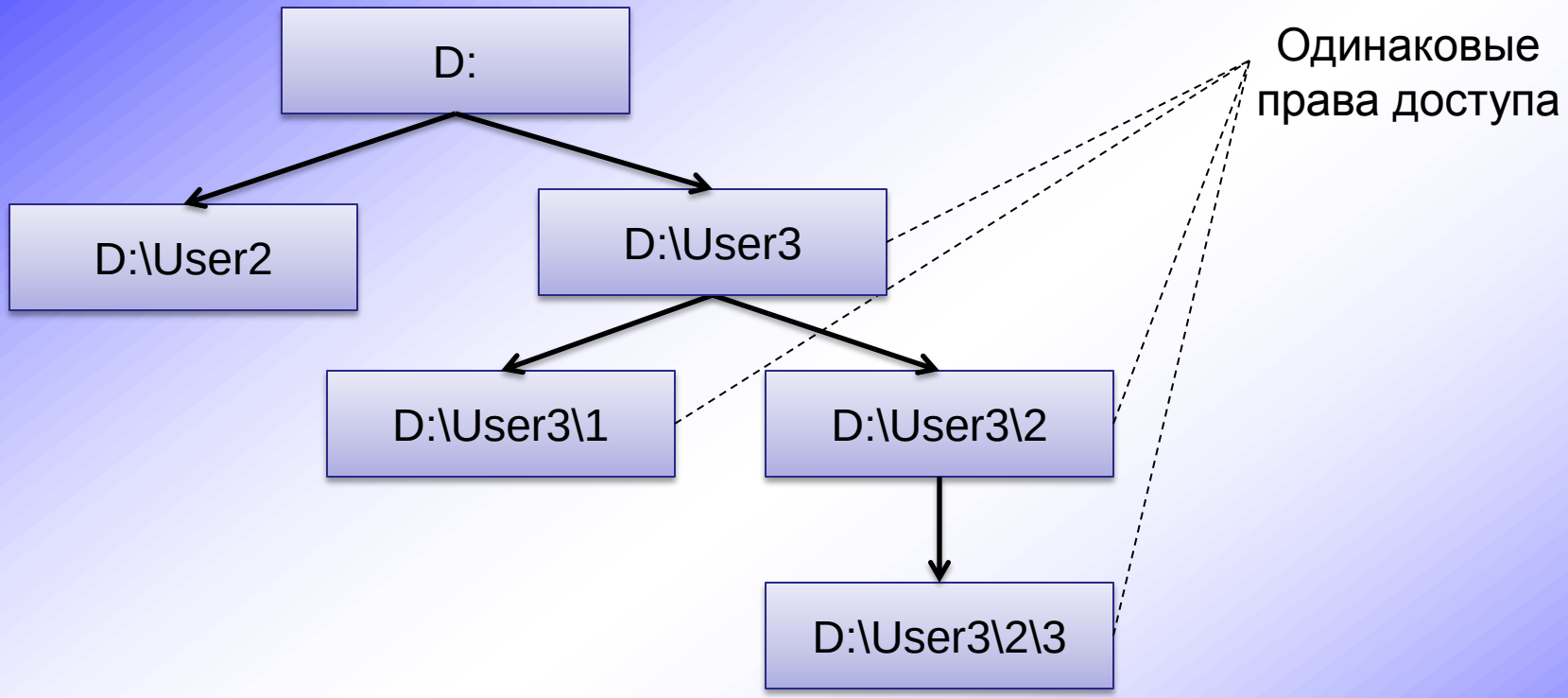
- правил, наследованных от родительских объектов;
- правил, явно заданных для этого объекта.

Реализация механизма наследования прав доступа

Для каждого объекта иерархии существует возможность:

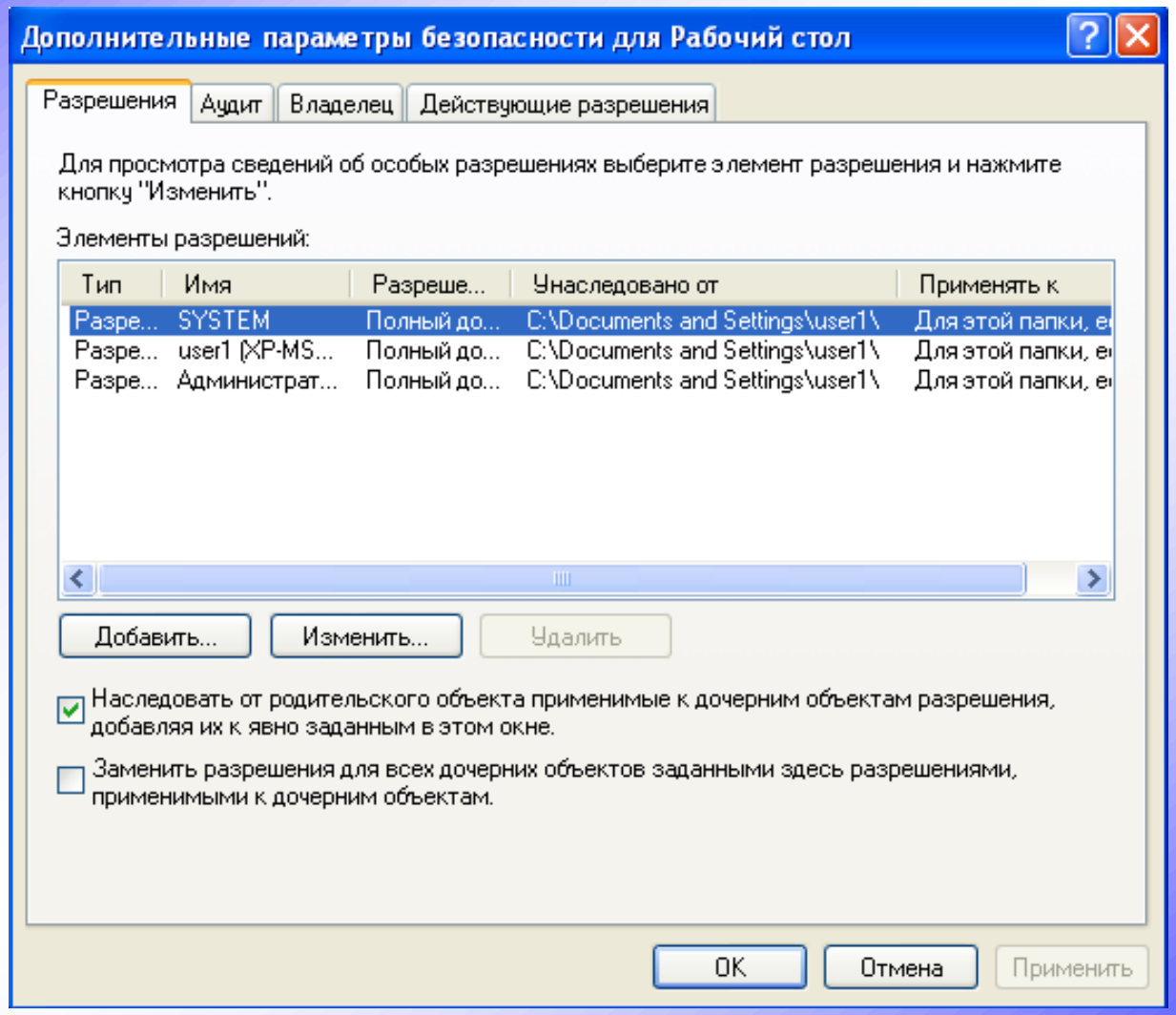
- установить/отключить наследование правил от родительского объекта;
- установить/отключить наследование правил этого объекта дочерними объектами;
- задать правила непосредственно для этого объекта.

Наследование разрешений

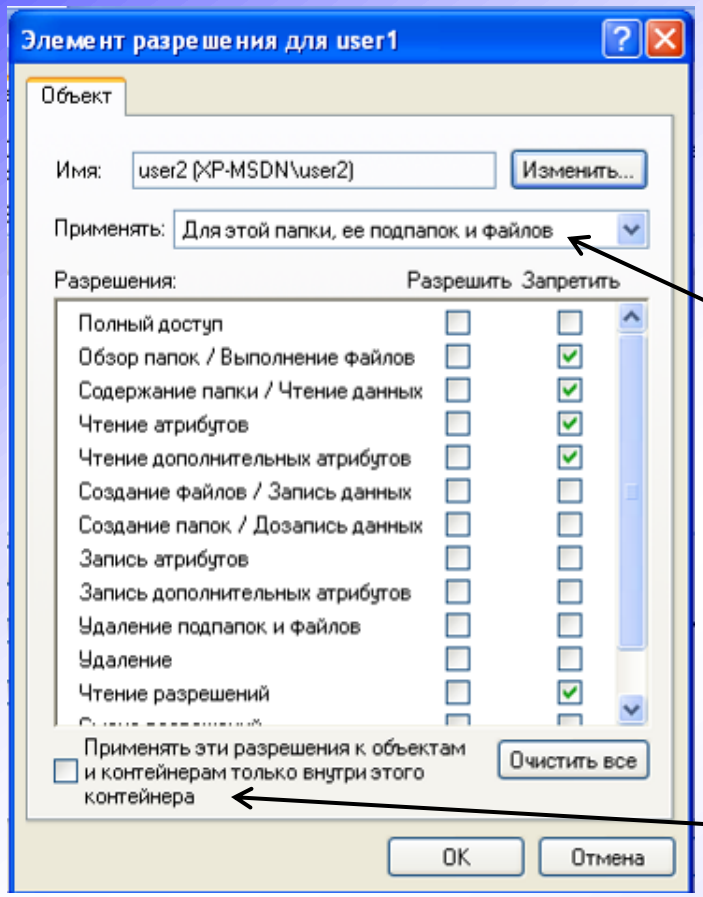


Если дочерним объектам необходимо применить те же права доступа, что и к родительскому, то можно использовать механизм наследования разрешений.

Наследование разрешений



Наследование разрешений



При задании правил для текущего объекта существует возможность:

- установить эти правила для самого объекта и для дочерних объектов (вложенных папок и файлов);
- определить способ наследования этих правил (для вложенных непосредственно в этот объект или для всех дочерних объектов).

Наследование разрешений

Применяется / Применять	Для текущей папки	Для подпапок текущей папки	Для файлов в текущей папке	Для всех вложенных подпапок	Для файлов во всех вложенных подпапках
Только для этой папки	да				
Для этой папки, её подпапок и файлов	да	да	да	да	да
Для этой папки и её подпапок	да	да		да	
Для этой папки и её файлов	да		да		да
Только для подпапок и файлов		да	да	да	да
Только для подпапок		да		да	
Только для файлов			да		да

Правила приоритета одного правила над другим

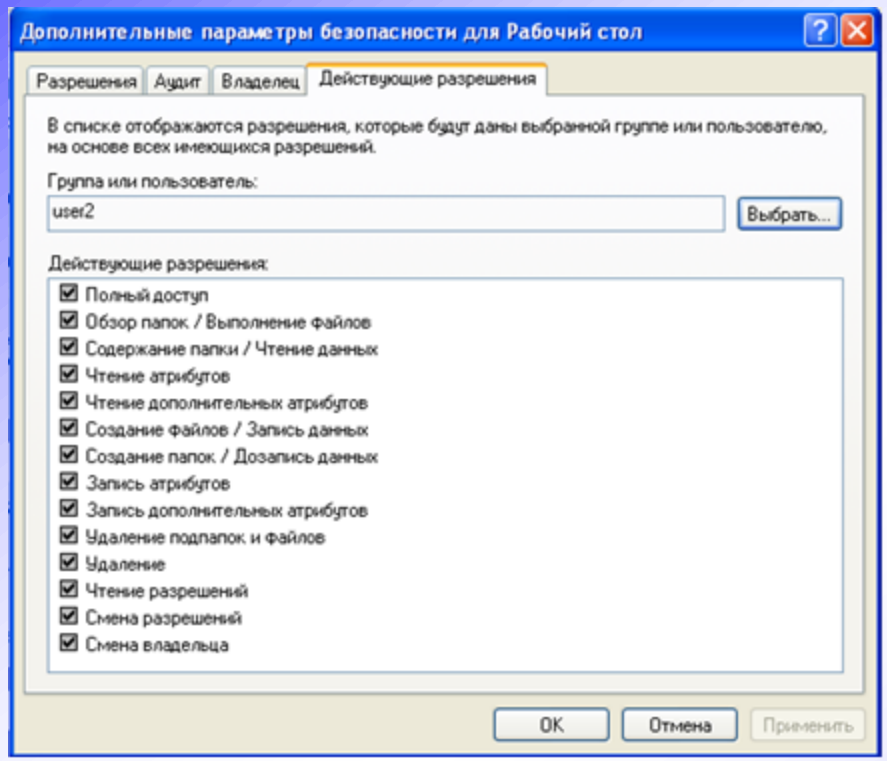
В случае конфликта разных правил (для одного субъекта установлены разные права, в т.ч. противоположные):

- на любом данном уровне разрешения от нескольких групп объединяются (например, право «Чтение» одного правила и право «Запись» другого правила);
- на любом данном уровне отрицательные разрешения (запреты) имеют приоритет над положительными;

Правила приоритета одного правила над другим

- разрешения, предоставленные объекту напрямую, имеют приоритет над наследуемыми разрешениями;
- разрешения, унаследованные от «близких родственников», имеют приоритет над разрешениями, унаследованными от «дальних родственников».

Действующие разрешения доступа пользователя к объекту



Для определения действующих разрешений конкретного субъекта (группы) по отношению к конкретному объекту с учётом правил приоритета и наследования в свойствах объекта существует вкладка «Действующие разрешения».

Рассмотренные вопросы

- Классификация субъектов и объектов доступа.
- Модели полномочного управления доступом с произвольным и принудительным управлением каналами взаимодействия пользователей.
- Правила разграничения доступа к иерархическим объектам.
- Правила наследования разрешений объектами.

Всем спасибо – все свободны,

если нет вопросов