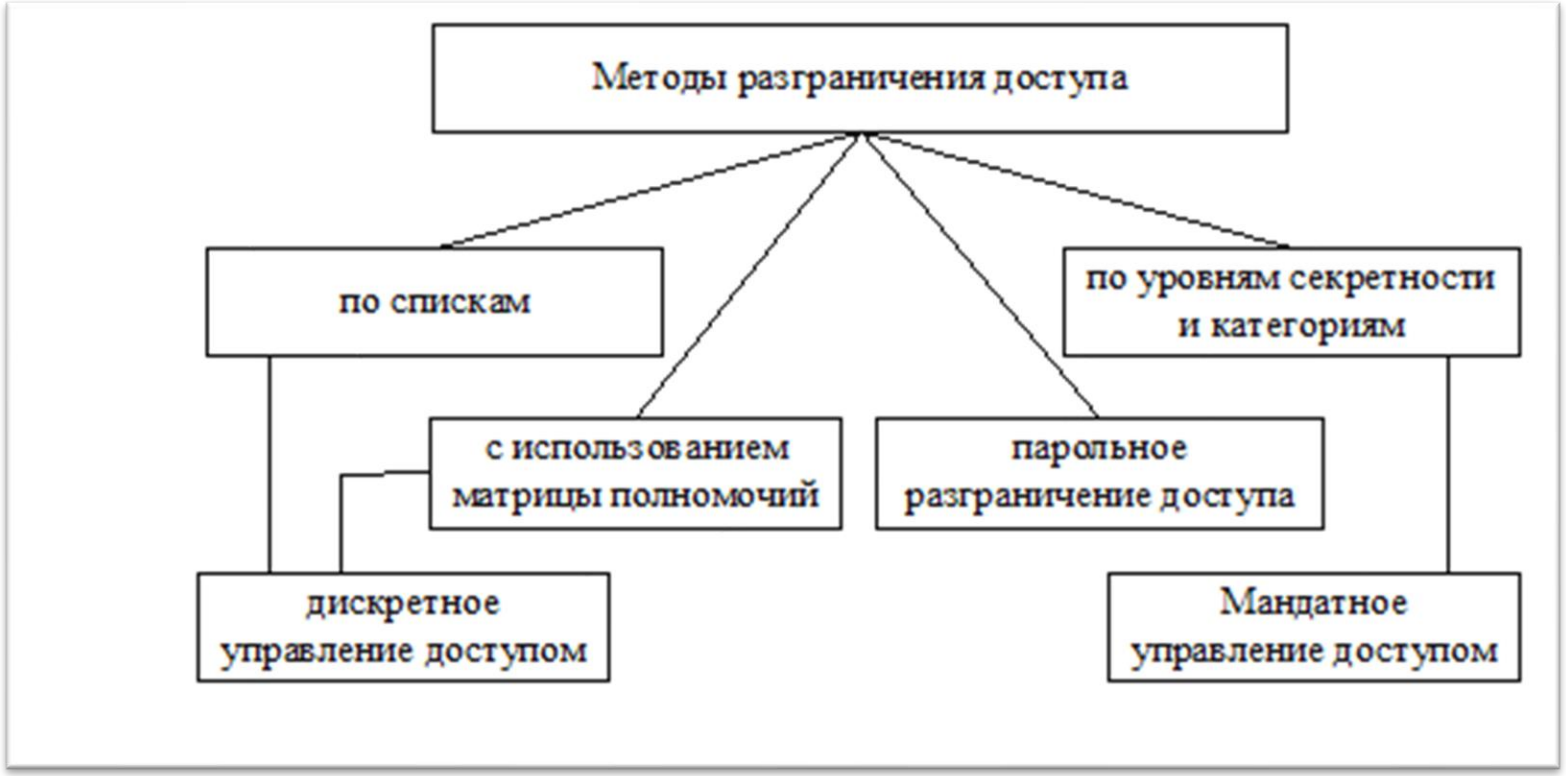
Разграничение доступа

Томчук Григорий Сергеевич
grigorijtomczuk@gmail.com

Разграничение доступа — совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы. Также данные правила называют *правами доступа* или *политиками безопасности*.

При разграничении доступа устанавливаются ***полномочия*** (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.



После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы. Обычно полномочия субъекта представляются: списком ресурсов, доступным пользователю и правами по доступу к каждому ресурсу из списка.

Существуют следующие методы разграничения доступа:

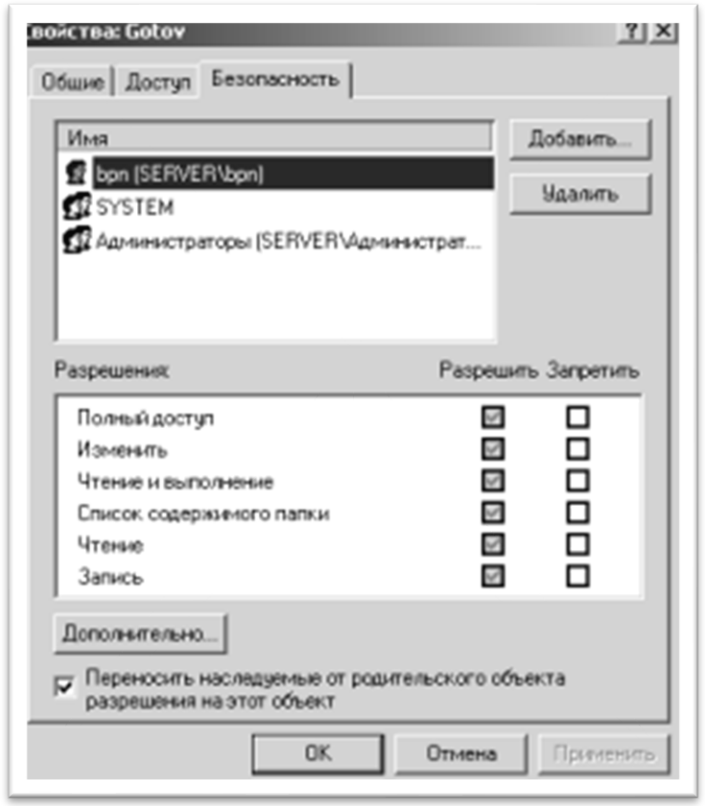
- *разграничение доступа по спискам;*
- *использование матрицы установления полномочий;*
- *разграничение доступа по уровням секретности и категориям;*
- *парольное разграничение доступа.*

Разграничение доступа по спискам

При разграничении доступа по спискам задаются соответствия: каждому пользователю — список ресурсов и прав доступа к ним или каждому ресурсу — список пользователей и их прав доступа к данному ресурсу

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Разграничение доступа по спискам



Пример (операционная система Windows 2000) разграничения доступа по спискам для одного объекта

Матрица установления полномочий

Использование матрицы установления полномочий подразумевает применение ***матрицы доступа*** (таблицы полномочий).

- В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в информационную систему, а столбцами — объекты (ресурсы) информационной системы.
- Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Матрица установления полномочий

Данный метод предоставляет более унифицированный и удобный подход, т.к. вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток — пустые).

Субъект	Диск C:\	Файл D:\prog.exe	Принтер
Пользователь 1	Чтение Запись Удаление	Выполнение Удаление	Печать Настройка параметров
Пользователь 2	Чтение	Выполнение	Печать 9:00 до 17:00
Пользователь 3	Чтение Запись	Выполнение	Печать с 17:00 до 9:00

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».

По уровням секретности и категориям

- 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.
- В качестве примера, где используются категории пользователей, приведем операционную систему Windows 2000, подсистема безопасности которой по умолчанию поддерживает следующие категории (группы) пользователей: «администратор», «опытный пользователь», «пользователь» и «гость». Каждая из категорий имеет определенный набор прав.
- Применение категорий пользователей позволяет упростить процедуры назначения прав пользователей за счет применения *групповых политик безопасности*.

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*.

Ограничение доступа к конкретным ресурсам

Если вы не хотите, чтобы кто-то имел доступ к конкретным ресурсам (социальным сетям, запрещенным сайтам), существует 3 доступных способа это сделать:

- *Запретить доступ локально на конкретном ПК*.
- *Настройка ACL (Access Control List) на граничном маршрутизаторе*. Смысл заключается в запрете доступа из конкретной подсети, к конкретным адресам.
- *Настройка DNS (Domain Name System) сервера*. Суть метода, в запрете разрешения конкретных доменных имен. Это означает, что при вводе в адресную строку браузера сайта vk.com, например, данное доменное имя не будет преобразовано в IPv4 адрес, и пользователь не сможет зайти на этот сайт.

Кратко

Определение полномочий (совокупность прав) субъекта для последующего контроля санкционированного использования им объектов информационной системы осуществляется после выполнения идентификации и аутентификации в подсистеме защиты.

Существуют следующие методы разграничения доступа:

- разграничение доступа по спискам;
- использование матрицы установления полномочий;
- разграничение доступа по уровням секретности и категориям;
- парольное разграничение доступа.

Кратко

- При разграничении доступа по спискам задаются соответствия: каждому пользователю — список ресурсов и прав доступа к ним или каждому ресурсу — список пользователей и их прав доступа к данному ресурсу.
- Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в информационную систему, а столбцами — объекты (ресурсы) информационной системы.

Кратко

- 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.
- Парольное разграничение основано на использовании пароля доступа субъектов к объектам.

Вопросы для закрепления

1. Как осуществляется разграничение доступа по уровням секретности и категориям?
2. Что называется разграничением доступа?
3. Как осуществляется разграничение доступа по спискам?