РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

Митюшин Дмитрий Алексеевич

Защита информации от несанкционированного доступа

Тема 4. Управление доступом к ресурсам

Вопросы:

1. *Механизмы управления доступом*
2. *Базовые модели доступа*
3. *Определение и классификация задач, решаемых механизмами управления доступом к ресурсам*

Литература

1. Щеглов А.Ю. Защита информации от несанкционированного доступа. – СПб.: Наука и техника. 2004. – 383 с

1. Механизмы управления доступом

Существует четыре основных способа разделения доступа субъектов к совместно используемым объектам:

Физическое – субъекты обращаются к физически различным объектам (однотипным устройствам, наборам данных на разных носителях и т.д.).

Временное – субъекты с различными правами доступа к объекту получают его в различные промежутки времени.

Логическое – субъекты получают доступ к совместно используемому объекту в рамках единой операционной среды, но под контролем средств разграничения доступа, которые моделируют виртуальную операционную среду «один субъект-все объекты»; в этом случае разделение может быть реализовано различными способами: разделение оригинала объекта, разделение с копированием объекта и т.д.

Криптографическое – все объекты хранятся в зашифрованном виде, права доступа определяются наличием ключа для расшифрования объекта.

1. Механизмы управления доступом

Механизмы управления доступом являются основой защиты ресурсов, обеспечивая решение задачи разграничения доступа субъектов к защищаемым информационным и техническим ресурсам – объектам.

В качестве субъектов в простейшем случае понимается пользователь.

На практике наличие механизмов управления доступом необходимо, даже если в системе может находиться только один прикладной пользователь.

Это вызвано тем, что, как правило, в системе должен быть также заведён пользователь с правами администратора, который настраивает параметры системы защиты и права доступа к ресурсам защищаемого объекта.

При этом у администратора принципиально иные права, чем у прикладного пользователя. Обо всем этом мы уже говорили.

1. Механизмы управления доступом

1.1. Абстрактные модели доступа

Механизм управления доступом реализует на практике некоторую абстрактную (или формальную) модель [3, 4, 8], определяющую ПРД к защищаемым ресурсам и правила обработки запросов доступа к защищаемым ресурсам.

Модель Биба

Одной из первых моделей была опубликованная в 1977 модель Биба (Biba). Согласно этой модели все субъекты и объекты предварительно разделяются по нескольким уровням доступа. Субъекты выполняют над объектами операции «читать» и «записывать».

Модель Биба определяет два правила, при соблюдении которых система гарантированно будет находиться в безопасном состоянии.

Простая аксиома целостности (*The Simple Integrity Axiom*) – субъекту данного уровня целостности запрещено выполнять операцию «читать» по отношению к объектам более низкого уровня целостности (правило «*no read down*»). Субъект, читая данные из объекта, характеризуемого более низким уровнем целостности, рискует «испортить» данные своего уровня, сделать их менее достоверными, поэтому такие операции должны быть запрещены. Зато он может читать проверенную, более достоверную информацию с более высоких уровней.

1. Механизмы управления доступом

1.1. Абстрактные модели доступа

Аксиома *-целостности (*The *-Integrity Axiom*) – субъекту данного уровня целостности запрещено выполнять операцию «записывать» по отношению к объектам более высокого уровня целостности (правило «*no write up*»).

Субъект, доверие к которому ограничивается некоторым уровнем целостности, не должен иметь возможность записывать данные в объекты более высокого уровня, так как он сможет внести в них искажения, неточности и тем самым снизить безопасность системы. Поток данных субъекта, направленный «вниз», не может ухудшить степень целостности объектов, имеющих более низкий уровень целостности.

Эта модель очень напоминает ограничения, введённые в защищённом режиме микропроцессоров Intel 80386+ относительно уровней привилегий.

Модель Гогена-Мезигера

Модель Гогена-Мезигера (Goguen-Meseguer), представленная ими в 1982 году, основана на теории автоматов. Согласно этой модели система может при каждом действии переходить из одного разрешённого состояния только в несколько других. Субъекты и объекты в данной модели защиты разбиваются на группы – домены.

1. Механизмы управления доступом

1.1. Абстрактные модели доступа

Переход системы из одного состояния в другое выполняется только в соответствии с так называемой таблицей разрешений, в которой указано, какие операции может выполнять субъект, например, из домена C над объектом из домена D.

В данной модели при переходе системы из одного разрешённого состояния в другое используются транзакции, что обеспечивает общую целостность системы.

Сазерлендская модель

Сазерлендская (от англ. Sutherland) модель защиты, опубликованная в 1986 году, основана на взаимодействии субъектов и потоков информации.

Также как и в предыдущей модели, здесь используется машина состояний со множеством разрешённых комбинаций состояний и некоторым набором начальных позиций. В данной модели исследуется поведение множественных композиций функций перехода из одного состояния в другое.

1. Механизмы управления доступом

1.1. Абстрактные модели доступа

Модель Кларка-Вильсона

Важную роль в теории защиты информации играет модель защиты Кларка-Вильсона (Clark-Wilson), опубликованная в 1987 году и модифицированная в 1989. Основана данная модель на повсеместном использовании транзакций и тщательном оформлении прав доступа субъектов к объектам.

В данной модели впервые исследована защищённость третьей стороны – стороны, поддерживающей всю систему безопасности. Эту роль в информационных системах обычно играет программа-супервизор.

Кроме того, в модели Кларка-Вильсона транзакции впервые были построены по методу верификации, то есть идентификация субъекта производилась не только перед выполнением команды от него, но и повторно после выполнения. Это позволило снять проблему подмены субъекта в момент между его идентификацией и собственно командой.

Модель Кларка-Вильсона считается одной из самых совершенных в отношении поддержания целостности информационных систем.

1. Механизмы управления доступом

1.1. Абстрактные модели доступа

Дискреционная (матричная) модель

Рассмотрим так называемую матричную модель защиты (её ещё называют дискреционной моделью), получившую на сегодняшний день наибольшее распространение на практике.

В терминах матричной модели, состояние системы защиты описывается следующей тройкой:

(S, O, M),

где S – множество субъектов, являющихся активными структурными элементами модели;
O – множество объектов доступа, являющихся пассивными защищаемыми элементами модели. Каждый объект однозначно идентифицируется с помощью имени объекта;
M – матрица доступа.

Значение элемента матрицы M [S, O} определяет права доступа субъекта S к объекту O.

Права доступа регламентируют способы обращения субъекта S к различным типам объектов доступа. В частности, права доступа субъектов к файловым

1. Механизмы управления доступом

1.1. Абстрактные модели доступа

Многоуровневые (мандатные) модели

С целью устранения недостатков матричных моделей были разработаны так называемые многоуровневые модели защиты, классическими примерами которых являются модель конечных состояний Белла и Ла-Падулы, а также решетчатая модель Д. Деннинг.

Многоуровневые модели предполагают формализацию процедуры назначения прав доступа посредством использования так называемых меток конфиденциальности или ***мандатов***, назначаемых субъектам и объектам доступа.

Так, для субъекта доступа метки, например, могут определяться в соответствии с уровнем допуска лица к информации, а для объекта доступа (собственно данные) – признаками конфиденциальности информации.

Признаки конфиденциальности фиксируются в метке объекта.

В связи с использованием терминов «мандат», «метка», «полномочия» много-уровневую защиту часто называют соответственно либо мандатной защитой, либо защитой с метками конфиденциальности, либо полномочной защитой.

2. Базовые модели доступа

Безопасность обработки информации обеспечивается путём решения задачи управления доступом субъектов к объектам в соответствии с заданным набором правил и ограничений, которые образуют политику безопасности или ПРД.

Можно выделить три основные модели управления доступом к объектам: дискреционную, мандатную и ролевую.

Но прежде разберёмся с понятиями «владелец» и «собственник» информации, т. к. при исследовании проблем управления доступом к ресурсам их трактовка является принципиальным моментом.

2. Базовые модели доступа

2.1. Понятия «владелец» и «собственник» информации

Сформулируем эти понятия, исходя из формализованных требований к механизмам защиты, а также из принципов реализации встроенной защиты в современных универсальных ОС.

На сегодняшний день в качестве «владельца» информации рассматривается либо пользователь, либо некое ответственное лицо. В качестве последнего, как правило, выступает сотрудник подразделения безопасности, в частности, администратор безопасности.

Здесь же отметим, что в существующих ОС пользователь сам может устанавливать атрибуты на создаваемые ими файловые объекты и не во всех случаях данные действия пользователя могут осуществляться в рамках задаваемых администратором ПРД.

Таким образом, в рамках существующих ОС «владелец» объекта файловой системы – это лицо, которое может устанавливать права доступа (атрибуты) к данному файловому объекту. В общем случае это может быть либо администратор, либо пользователь, создающий файловый объект.

2. Базовые модели доступа

2.1. Понятия «владелец» и «собственник» информации

Однако права «владельца» в конечном счёте, определяются тем, кто является собственником информации, т.к. именно собственник информации может принимать решение о её передаче другим лицам.

Естественно, что когда речь идёт о домашнем компьютере, то собственником и «владельцем» является непосредственный хозяин компьютера, обрабатывающий на нём собственную информацию.

Другое дело – применение СВТ и АС на предприятии. Использование защищаемого компьютера на предприятии, как правило, связано с защитой служебной информации, конфиденциальных данных и т.д. Но эта информация уже не является собственностью пользователя, следовательно, не пользователь должен являться её конечным «владельцем».

При этом также необходимо учитывать, что, по статистике, большинство хищений информации на предприятии (умышленно или нет) осуществляется непосредственно сотрудниками, в частности, пользователями защищаемых компьютеров. Естественно, то же (но в большей мере) относится к защите секретной информации, собственником которой является государство.

2. Базовые модели доступа

2.1. Понятия «владелец» и «собственник» информации

В общем случае, владельцем служебной информации является предприятие.

Что касается конфиденциальной информации, то здесь все зависит от её типа.

В связи с этим большинство приложений систем защиты связано именно с защитой данных, собственником которых пользователь не является.

Отметим, что в основу рассматриваемой далее разграничительной политики доступа должен быть положен следующий тезис:

Пользователь не является собственником обрабатываемой им информации, как следствие, не может рассматриваться её «владельцем», т.е. не должен иметь прав назначать и изменять ПРД к объектам файловой системы.

«Владельцем» объектов файловой системы должен рассматриваться администратор безопасности, являющийся ответственным лицом собственника, в частности, предприятия.

2. Базовые модели доступа

2.2. Дискреционное разграничение доступа

Система правил дискреционного (избирательного) разграничения доступа формулируется следующим образом.

1. Для любого объекта существует владелец.
2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой тройки субъект-объект-метод возможность доступа определена однозначно.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу доступа.

Привилегированный пользователь не может игнорировать разграничение доступа к объектам. Например, в Windows NT администратор для обращения к чужому объекту (принадлежащему другому субъекту) должен сначала объявить себя владельцем этого объекта, использовав привилегию администратора, объявлять себя владельцем любого объекта, затем дать себе необходимые права и только после этого может обратиться к объекту.

2. Базовые модели доступа

2.2. Дискреционное разграничение доступа

При создании объекта его владельцем назначается субъект, создавший данный объект. В дальнейшем субъект, обладающий необходимыми правами, может назначить объекту нового владельца. При этом субъект, изменяющий владельца объекта, может назначить новым владельцем объекта только себя. Такое ограничение вводится для того, чтобы владелец объекта не мог отдать «владение» объектом другому субъекту и тем самым снять с себя ответственность за некорректные действия с объектом.

Для определения прав доступа субъектов к объектам при избирательном разграничении доступа используются такие понятия, как ***матрица доступа*** и ***домен безопасности***.

Домен безопасности (*protection domain*) определяет набор объектов и типов операций, которые могут производиться над каждым объектом ОС.
Возможность выполнять операции над объектом есть право доступа, каждое из которых есть упорядоченная пара <object-name, rights-set>. Таким образом, домен есть набор прав доступа. Например, если домен D имеет право доступа <file F, (read, write)>, это означает, что процесс, выполняемый в домене D, может читать или писать в файл F, но не может выполнять других операций над этим объектом (рис. 1).

2. Базовые модели доступа

2.2. Дискреционное разграничение доступа

Объект / Домен	**F1**	**F2**	**F3**	**Printer**
D1	read		execute	
D2		read		
D3				print
D4	read write		read write	

Рис. 1. Специфицирование прав доступа к ресурсам

2. Базовые модели доступа

2.2. Дискреционное разграничение доступа

Связь конкретных субъектов, функционирующих в АС, может быть организована следующим образом:

- каждый пользователь может быть доменом. В этом случае набор объектов, к которым может быть организован доступ, зависит от идентификации пользователя;
- каждый процесс может быть доменом. В этом случае набор доступных объектов определяется идентификацией процесса;
- каждая процедура может быть доменом. В этом случае набор доступных объектов соответствует локальным переменным, определённым внутри процедуры. Заметим, что, когда процедура выполнена, происходит смена домена.

Модель безопасности, специфицированная выше (см. рис. 1), имеет вид матрицы и называется ***матрицей доступа***. Столбцы этой матрицы представляют собой объекты, строки – субъекты. В каждой ячейке матрицы хранится совокупность прав доступа, предоставленных данному субъекту на данный объект.

Поскольку реальная матрица доступа очень велика (типичный объём для современной АС составляет несколько десятков мегабайтов), матрицу доступа никогда не хранят в системе в явном виде. В общем случае эта матрица будет

2. Базовые модели доступа

2.2. Дискреционное разграничение доступа

Матрицу доступа можно разложить по столбцам, в результате чего получаются ***списки прав доступа ACL*** (*access control list*). В результате разложения матрицы по строкам получаются мандаты возможностей (*capability list*, или *capability tickets*).

Список прав доступа ACL. Каждая колонка в матрице может быть реализована как список доступа для одного объекта. Очевидно, что пустые клетки могут не учитываться. В результате для каждого объекта имеем список упорядоченных пар <domain, rights-set>, который определяет все домены с непустыми наборами прав для данного объекта.

Элементами списка прав доступа ACL могут быть процессы, пользователи или группы пользователей. При реализации широко применяется предоставление доступа по умолчанию для пользователей, права которых не указаны. Например, в ОС Unix все субъекты-пользователи разделены на три группы (владелец, группа и остальные), и для членов каждой группы контролируются операции чтения, записи и исполнения (rwx). В итоге имеем ACL – 9-битный код, который является атрибутом разнообразных объектов Unix.

2. Базовые модели доступа

2.2. Дискреционное разграничение доступа

Мандаты возможностей. Как отмечалось выше, если матрицу доступа хранить по строкам, т.е. если каждый субъект хранит список объектов и для каждого объекта – список допустимых операций, то такой способ хранения называется «мандаты возможностей» или «перечни возможностей» (*capability list*).

Каждый пользователь обладает несколькими мандатами и может иметь право передавать их другим. Мандаты могут быть рассеяны по системе и вследствие этого представлять большую угрозу для безопасности, чем списки контроля доступа. Их хранение должно быть тщательно продумано.

Дискреционная модель – наиболее распространённый способ разграничения доступа. Это обусловлено сравнительной простотой его реализации и необременительностью правил такого разграничения доступа для пользователей. Главное достоинство – гибкость; основные недостатки – рассредоточенность управления и сложность централизованного контроля.

Вместе с тем, защищённость ОС, подсистема защиты которой реализует только избирательное разграничение доступа, в некоторых случаях может оказаться недостаточной. В частности, в США запрещено хранить информацию, содержащую государственную тайну, в компьютерных системах, поддерживающих только дискреционное разграничение доступа

2. Базовые модели доступа

2.2. Дискреционное разграничение доступа

Расширением модели дискреционного разграничения доступа является ***изолированная*** (или ***замкнутая***) ***программная*** среда.

При использовании изолированной программной среды права субъекта на доступ к объекту определяются не только правами и привилегиями субъекта, но и процессом, с помощью которого субъект обращается к объекту.

Можно, например, разрешить обращаться к файлам с расширением .doc только программам Word, Word Viewer и WPview.

Изолированная программная среда существенно повышает защищённость операционной системы от разрушающих программных воздействий, включая программные закладки и компьютерные вирусы.

Кроме того, при использовании данной модели повышается защищённость целостности данных, хранящихся в системе.

2. Базовые модели доступа

2.3. Мандатное разграничение доступа

Мандатное разграничение доступа (*mandatory access control*) или полномочное разграничение доступа с контролем информационных потоков, обычно применяется в совокупности с дискреционной моделью. Рассмотрим именно такой случай. Правила разграничения доступа в данной модели формулируются следующим образом.

1. Каждому субъекту и объекту доступа должны сопоставляться классификационные метки, отражающие их место в соответствующей иерархии (метки конфиденциальности). Посредством этих меток субъектами объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.
2. Система защиты при вводе новых данных в систему должна запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта ему должны назначаться классификационные метки. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри системы защиты).

2. Базовые модели доступа

2.3. Мандатное разграничение доступа

3. Система защиты должна реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:
   - субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта. При этом иерархические категории в классификационном уровне субъекта должны включать в себя все иерархические категории в классификационном уровне объекта;
   - субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации. При этом все иерархические категории в классификационном уровне субъекта должны включаться в иерархические категории в классификационном уровне объекта.
4. Реализация мандатных ПРД должна предусматривать возможность сопровождения, изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

2. Базовые модели доступа

2.3. Мандатное разграничение доступа

5. В СВТ должен быть реализован диспетчер доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должны контролироваться не только единичный акт доступа, но и потоки информации.

При использовании данной модели разграничения доступа существенно страдает производительность АС, поскольку права доступа к объекту должны проверяться не только при открытии объекта, но и при каждой операции чтение/запись.

Кроме того, эта модель создаёт пользователям определённые неудобства: если уровень конфиденциальности процесса строго выше нуля, то вся информация в памяти процесса фактически является секретной и не может быть записана в несекретный объект.

Если процесс одновременно работает с двумя объектами, только один из которых является секретным, то он не может записывать информацию из памяти во второй объект. Эта проблема решается посредством использования специального программного интерфейса API для работы с памятью. Области памяти, выделяемые процессам, могут быть описаны как объекты мандатного разграничения доступа, после чего им могут назначаться грифы секретности

2. Базовые модели доступа

2.3. Мандатное разграничение доступа

При чтении секретного файла процесс должен считать содержимое такого файла в секретную область памяти, используя для этого функции ОС, гарантирующие невозможность утечки информации. Для работы с секретной областью памяти процесс также должен использовать специальные функции. Поскольку утечка информации из секретных областей памяти в память процесса невозможна, считывание процессом секретной информации в секретные области памяти не отражается на уровне конфиденциальности процесса. Если же процесс считывает секретную информацию в область памяти, не описанную как объект мандатного разграничения доступа, повышается уровень конфиденциальности процесса.

Каждая из рассмотренных моделей разграничения доступа имеет свои достоинства и недостатки.

В большинстве ситуаций применение дискреционного разграничения доступа наиболее эффективно. Изолированную программную среду целесообразно использовать в случаях, когда важно обеспечить целостность программ и данных ОС. Мандатное разграничение доступа с контролем информационных потоков следует применять в тех случаях, когда для организации чрезвычайно важно обеспечение защищённости системы от НСД. В остальных ситуациях применение этой модели нецелесообразно из-за резкого ухудшения эксплуатационных качеств ОС.

2. Базовые модели доступа

2.4. Ролевая модель разграничения доступа

В системах компьютерной безопасности, контролем доступа на основе ролей (*RBAC, – role-based access control*) называется способ построения систем разграничения доступа авторизованных пользователей.

С недавних пор он является альтернативой мандатному контролю доступа (*MAC – mandatory access control*) и дискреционному контролю доступа (*DAC – discretionary access control*).

Ролевая модель контроля доступа RBAC достаточно гибка и сильна, чтобы смоделировать как дискреционный, так и мандатный контроль доступа.

До разработки ролевой модели, единственными известными моделями контроля доступа были мандатная и дискреционная: если модель была не мандатная, то она была дискреционная, и наоборот. Ролевая модель не попадает ни в ту, ни в другую категорию.

Роли создаются внутри организации для различных рабочих функций. Определённым ролям присваиваются полномочия (*'permissions'*) для выполнения тех или иных операций.

2. Базовые модели доступа

2.4. Ролевая модель разграничения доступа

Штатным сотрудникам (или другим пользователям системы) назначаются фиксированные роли, через которые они получают соответствующие привилегии для выполнения фиксированных системных функций.

В отличие от контроля доступа на основе кон текста (CBAC, – *context-based access control*), ролевая модель не принимает во внимание текущую ситуацию (такую как, например, откуда было установлено соединение).

Так как привилегии не назначаются пользователям непосредственно, и приобретаются ими только через свою роль (или роли), управление индивидуальными правами пользователя по сути превращается в простое присвоение ему ролей. Это упрощает общие операции, такие как добавление пользователя или смена подразделения пользователем.

Ролевая модель отличается от списков контроля доступа (ACL, – *access control lists*), используемых в традиционных дискреционных системах контроля доступа тем, что может присваивать привилегии на сложные операции с составными данными, а не только на атомарные операции с низкоуровневыми объектами данных. Например, лист контроля доступа может предоставить или лишить права записи в такой-то системный файл, но он не может сказать, каким образом этот файл может быть изменён.

2. Базовые модели доступа

2.4. Ролевая модель разграничения доступа

Система, основанная на рассматриваемой, позволяет создать такую операцию как «открытие кредита» в финансовом приложении или заполнение записи «тест на уровень сахара в крови» в медицинском приложении. Присвоение привилегии на выполнение операции многозначно, так как операции являются дробящимися в пределах приложения.

Концепции иерархии ролей и ограничений позволяют создать или смоделировать контроль доступа на основе решётки (*LBAC, – lattice-based access control*) средствами ролевой модели. Таким образом, ролевая модель может быть основанием и расширением модели доступа на основе решётки.

Для определения ролевой модели используются следующие соглашения:
S = Субъект (*Subject*) = Человек или процесс
R = Роль (*Role*) = Рабочая функция или название, которое определяется на уровне авторизации
P = Разрешения (*Permissions*) = Одобрение режима доступа к ресурсу
SE = Сессия (*Session*) = Соответствие между S, R и/или P
SA = Назначение субъекта (*Subject Assignment*)
PA = Назначение разрешения (*Permission Assignment*)
RH = Частично упорядоченная иерархия ролей (*Role Hierarchy*). RH может быть ещё записана так: ≥ Обозначение: x ≥ y означает, что *x* наследует разрешения *y.*

2. Базовые модели доступа

2.4. Ролевая модель разграничения доступа

Один субъект может иметь несколько ролей.
Одну роль могут иметь несколько субъектов.
Одна роль может иметь несколько разрешений.
Одно разрешение может принадлежать нескольким ролям.

На возможность наследования разрешений от противоположных ролей накладывается ограничительная норма, которая позволяет достичь надлежащего разделения режимов. Например, одному и тому же лицу может быть не позволено создать учётную запись для кого-то, а затем авторизоваться под этой учётной записью.

Используя нотацию теории множеств:

$PA \subseteq P \times A$ при этом разрешения назначаются связям ролей в отношении «многие ко многим».

$SA \subseteq S \times A$ при этом субъекты назначаются связям ролей и субъектов в отношении «многие ко многим».

Субъект может иметь множество одновременных сессий с различными разрешениями.

2. Базовые модели доступа

2.4. Ролевая модель разграничения доступа

Ролевая модель широко используется для управления пользовательскими привилегиями в пределах единой системы или приложения. Это является наилучшей практикой.

Список таких систем включает в себя *Microsoft Active Directory*, *SELinux*, *FreeBSD*, *Solaris*, СУБД *Oracle*, *PostgreSQL* 8.1, *SAP* R/3 и множество других, эффективно применяющих RBAC.

В организациях с разнородной IT-инфраструктурой, в диапазоне от дюжины до сотен систем и приложений, следует создавать иерархию ролей и наследование привилегий. Без этого использование RBAC становится крайне запутанным.

Для больших систем с сотнями ролей, тысячами пользователей и миллионами разрешений управление ролями, пользователями, разрешениями и их взаимосвязями является сложной задачей, которую нереально выполнить малой группой администраторов безопасности.

Привлекательной возможностью является использование самой RBAC для содействия децентрализованному управлению RBAC.

2. Базовые модели доступа

2.5. Управление доступом на основе атрибутов

Одним из подходов повышения эффективности управления доступом является использование ***управления доступом на основе атрибутов*** (ABAC).

Этот подход использует анализ атрибутов субъектов и объектов доступа, а также времени и среды.

Доступ предоставляется на основе правил или политик, которые представляют из себя набор условий для проверки атрибутов, например:

Бизнес-Правило: «Менеджер может редактировать заказ, только если стоимость заказа не выше 1000 руб. и заказ находится в его филиале».

Включает в себя Условия:

- Субъект.Должность = "Менеджер"
- Объект.Тип = "Заказ"
- Действие.Название = "Редактирование"
- Объект.Филиал = "Субъект.Филиал"
- Объект.Стоимость < "1000"

2. Базовые модели доступа

2.5. Управление доступом на основе атрибутов

Главное преимущество над классическими моделями управления доступом – возможность использовать сложные правила с проверкой времени суток, дня недели, IP адреса, города, филиала и т.д. Это позволяет реализовать динамическую модель предоставления доступа гораздо более гибкую, чем при использовании, например, классического подхода ролевой модели.

Однако использование только лишь логики данной в реальной жизни приведёт к созданию множества сложных правил, где необходимо будет учитывать множество атрибутов и их значений, что может быть достаточно затратно. Правила необходимо поддерживать и обновлять. Такая модель становится сложноуправляемой и менее понятной, ведь отличие от ролевой модели, где в ролях хранятся наборы прав, данная не использует понятия права. Посмотрев на правила атрибутной модели нельзя сказать точно, какие привилегии у какого пользователя сейчас есть. Это значит, что данная модель не подходит для аудита прав пользователей.

Поэтому, все чаще гибкость атрибутной модели используется для расширения возможностей ролевой модели доступа. Например, создание более сложных правил ролевой модели, которые позволят сделать роли динамически назначаемыми. Есть и другие реализации, когда правила атрибутов ограничивают предоставленные ролью права. Подобные способы комбинирования подходами позволяют реализовать более удобные, понятные и легкоуправляемые модели управления доступом. Конечно же, выбор способа необходимо тщательно продумать в зависимости от конкретного случая.

2. Базовые модели доступа

2.6. Выбор модели

Следуя формализованным требованиям к системе защиты информации, основой реализации разграничительной политики доступа к ресурсам при обработке сведений конфиденциального характера является ***дискреционный механизм управления доступом***, а секретных сведений – ***мандатный***.

2. Базовые модели доступа

2.7. Дополнительные требования к защите секретной информации в контексте использования дискреционной и мандатной моделей управления доступом

При защите секретной информации используется и дискреционная и мандатная модели управления доступом. Требования к реализации мандатной модели в рамках защиты секретной информации были приведены в предыдущем пункте. Что касается требований к дискреционному механизму, то при защите секретной информации следует придерживаться тех же требований, что и для защиты конфиденциальной информации. Однако в дополнение к последним добавляется ещё пара требований:

- Система защиты должна содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД. Под «явными» подразумеваются действия, осуществляемые с использованием системных средств – системных макрокоманд, инструкций языков высокого уровня и т.д. Под «скрытыми» – иные действия, в том числе с использованием злоумышленником собственных программ работы с устройствами.
- Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.

Кроме того, отдельно сформулированы требования к управлению доступом к устройствам.

2. Базовые модели доступа

2.8. Защита ввода и вывода на отчуждаемый физический носитель информации

- Система защиты должна различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»). При вводе с «помеченного» устройства (выведана «помеченное» устройство) система защиты должна обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с «помеченным» каналом связи.
- Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем системы защиты.

2. Базовые модели доступа

2.9. Сопоставление пользователя с устройством

- Система защиты должна обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так для идентифицированных (при совпадении маркировки).
- Система защиты должна включать в себя механизм, посредством которого санкционированный пользователь надёжно сопоставляется с выделенным ему конкретным устройством.

3. Классификация объектов и субъектов доступа к ресурсам

3.1. Корректность и полнота реализации разграничительной политики доступа

Для механизмов управления доступом подход, что пользователь не является «владельцем» обрабатываемой им информации связан с понятиями корректности и полноты реализации разграничительной политики доступа к ресурсам.

Под ***корректностью реализации разграничительной политики доступа*** к ресурсу будем понимать свойство механизма управления доступом полностью разделять ресурс между пользователями системы.

При этом разграничение доступа должно быть реализовано так, чтобы разные пользователи имели доступ к непересекающимся элементам разделяемого ресурса, т.е. чтобы обеспечивалась невозможность несанкционированного обмена ими информацией между собой посредством данного ресурса.

Под ***полнотой реализации разграничительной политики доступа к*** ресурсам будем понимать свойство системы защиты обеспечивать корректную реализацию разграничительной политики доступа ко всем ресурсам системы, посредством которых возможен несанкционированный обмен информацией пользователей между собой.

Данные определения вытекают из рассмотренных выше формализованных

3. Классификация объектов и субъектов доступа к ресурсам

3.1. Корректность и полнота реализации разграничительной политики доступа

Очевидно, что требование к полноте разграничений доступа к ресурсам может выполняться только в том случае, когда доверенным лицом владельца информации (предприятия, либо государства) выступает не пользователь, а некий субъект, внешний по от ношению к информации, обрабатываемой на защищаемом компьютере.

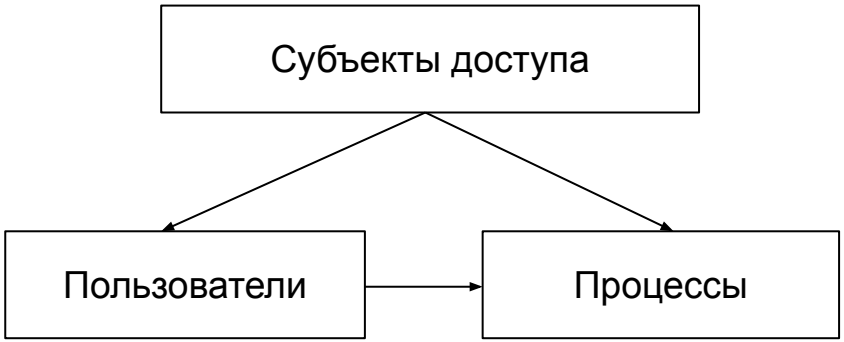
Этот субъект наделяется специальными полномочиями и обладает необходимым элементом доверия со стороны владельца информации (в частности, предприятия). Таким субъектом и является администратор безопасности.

3. Классификация объектов и субъектов доступа к ресурсам

3.2. Общая классификация субъектов и объектов доступа

Немаловажным является вопрос классификации субъектов и объектов доступа. Именно на основе этой классификации определяются задачи, которые должны решаться механизмами управления доступом. При этом разграничивается доступ каждого субъекта к каждому объекту.

Прежде всего, введём общую классификацию субъектов и объектов доступа, которые потенциально могут присутствовать в защищаемой системе. Общая классификация субъектов доступа приведена на рис. 2

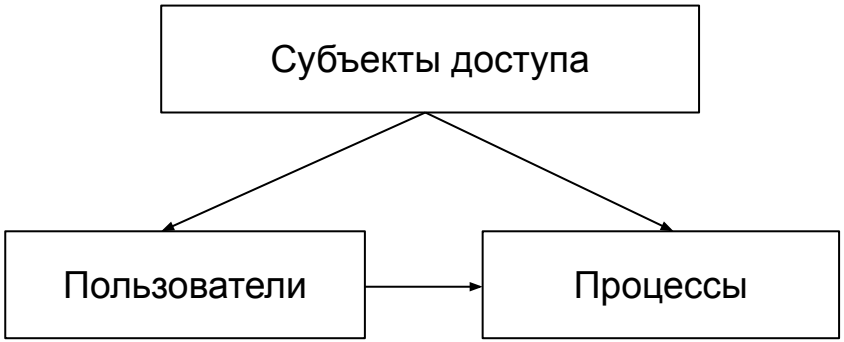


Общая классификация субъектов доступа

3. Классификация объектов и субъектов доступа к ресурсам

3.2. Общая классификация субъектов и объектов доступа

Горизонтальная связь на рис. 2 отражает, что субъекты «ПОЛЬЗОВАТЕЛЬ» и «ПРОЦЕСС» не могут рассматриваться независимо, т.к. запрос доступа к ресурсу генерирует процесс, запускаемый пользователем.

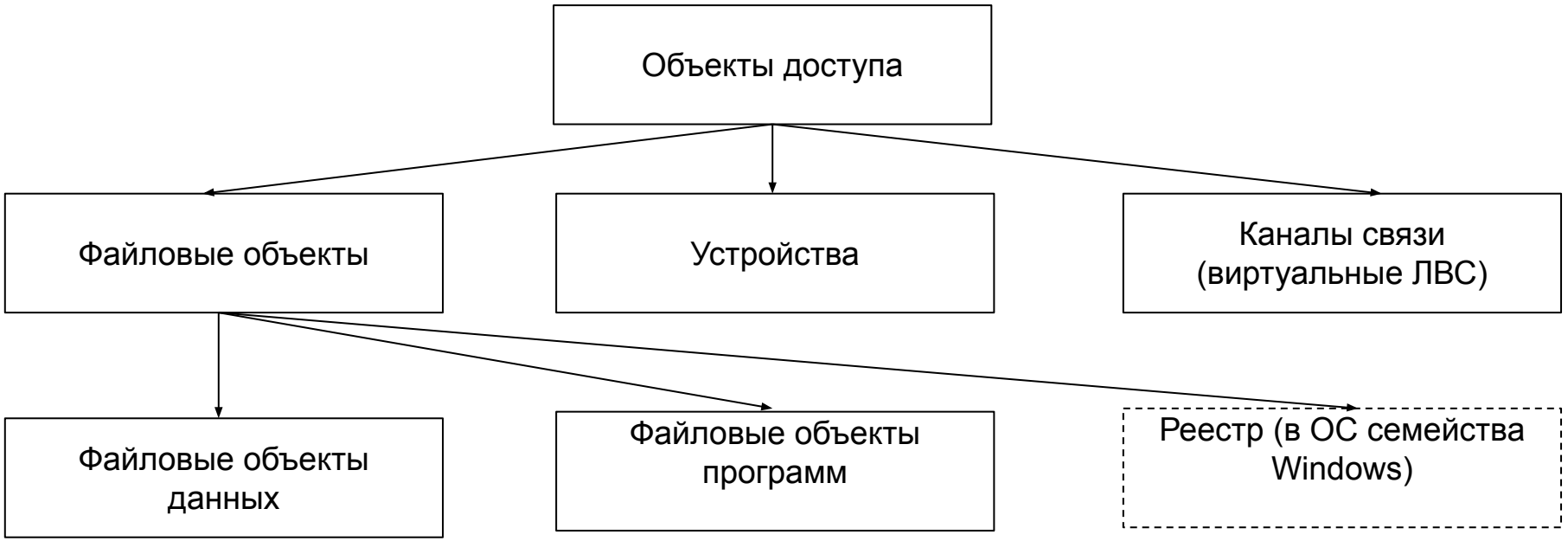


Общая классификация субъектов доступа

3. Классификация объектов и субъектов доступа к ресурсам

3.2. Общая классификация субъектов и объектов доступа

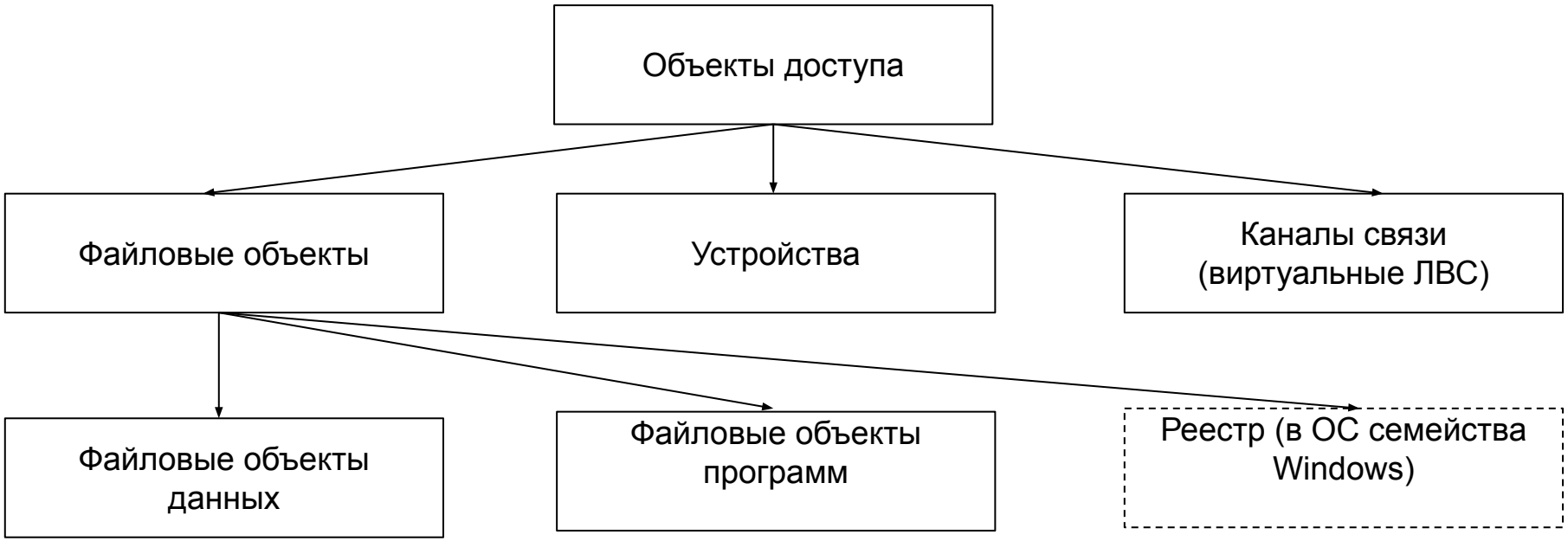
Общая классификация объектов доступа



3. Классификация объектов и субъектов доступа к ресурсам

3.2. Общая классификация субъектов и объектов доступа

Общая классификация объектов доступа



3. Классификация объектов и субъектов доступа к ресурсам

3.2. Общая классификация субъектов и объектов доступа

Очевидно, что представленные классификации содержат всю возможную совокупность субъектов и объектов доступа защищаемого компьютера.

Теперь введём детальные классификации возможных в системе субъектов и объектов доступа, доступ которых (к которым) должен разграничивать диспетчер доступа. Здесь же определим механизмы управления доступом, решающие задачи разграничения прав доступа.

3. Классификация объектов и субъектов доступа к ресурсам

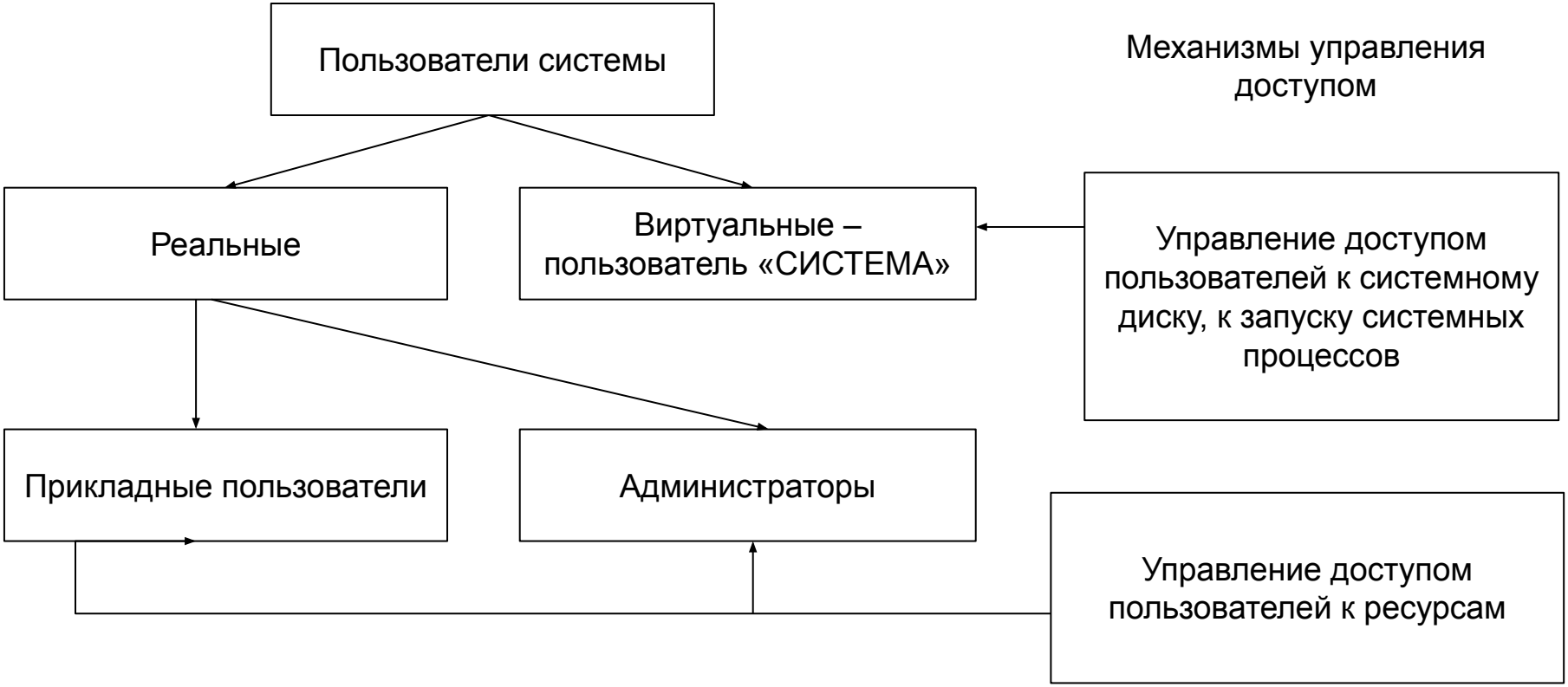
3.3. Детальная классификация субъектов доступа

Как отмечалось, субъектами доступа к ресурсам компьютера являются пользователи и процессы. При этом каждый из этих субъектов, в свою очередь, может быть классифицирован.

3. Классификация объектов и субъектов доступа к ресурсам

3.3. Детальная классификация субъектов доступа

Классификация пользователей.



3. Классификация объектов и субъектов доступа к ресурсам

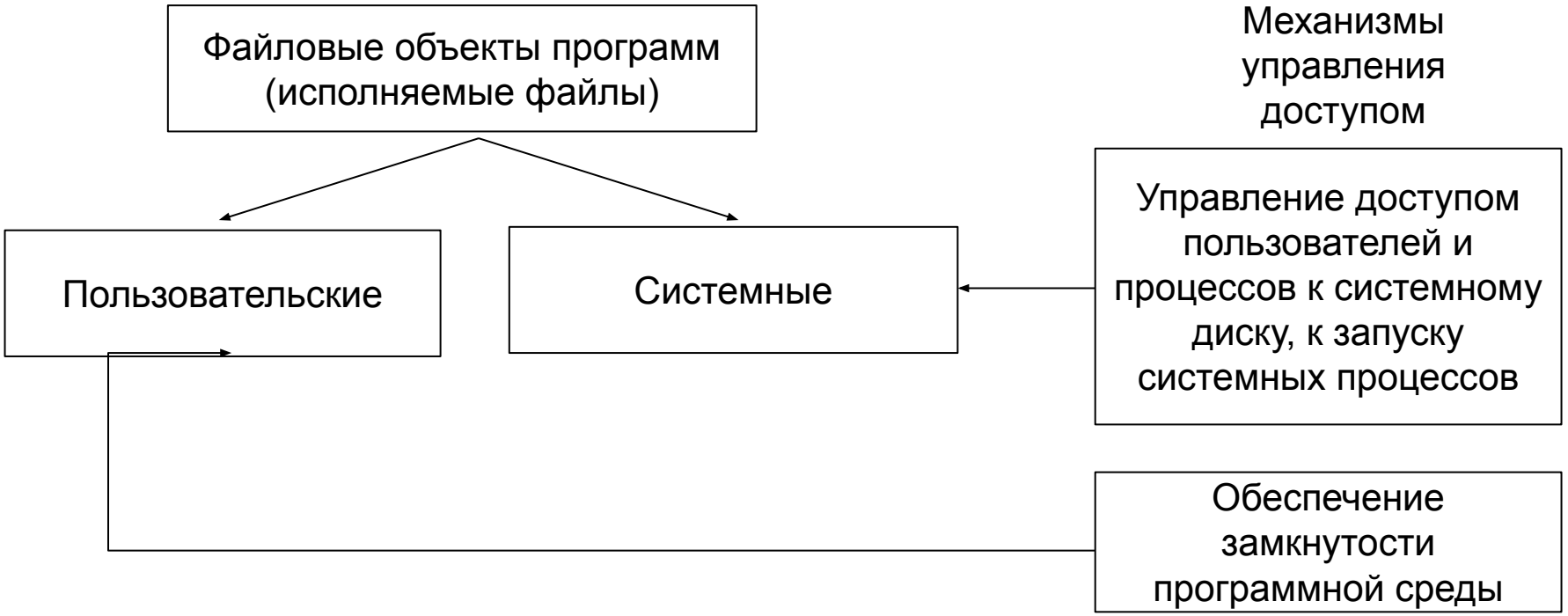
3.3. Детальная классификация субъектов доступа

Классификация процессов

3. Классификация объектов и субъектов доступа к ресурсам

3.3. Детальная классификация субъектов доступа

Классификация файловых объектов программ



3. Классификация объектов и субъектов доступа к ресурсам

3.3. Детальная классификация субъектов доступа

Классификация файловых объектов данных

3. Классификация объектов и субъектов доступа к ресурсам

3.3. Детальная классификация субъектов доступа

Классификация устройств

3. Классификация объектов и субъектов доступа к ресурсам

3.3. Детальная классификация субъектов доступа

Классификация каналов связи (виртуальные) ЛВС, в предположении, что защищаемый объект находится в составе ЛВС

3. Классификация объектов и субъектов доступа к ресурсам

3.3. Детальная классификация субъектов доступа

Классификация каналов связи (виртуальные) ЛВС, в предположении, что защищаемый объект находится в составе ЛВС

3. Классификация объектов и субъектов доступа к ресурсам

3.3. Детальная классификация субъектов доступа

С учётом сказанного можем сделать вывод о необходимости управления доступом для каждой пары «субъект-объект». Без этого не может быть обеспечена полнота разграничительной политики доступа к ресурсам защищаемого объекта.

При этом должна быть реализована следующая совокупность механизмов:

1. Механизм управления доступом пользователей (прикладных пользователей и администратора) к ресурсам.
2. Механизм управления доступом процессов (прикладных и системных) к ресурсам.
3. Механизм комбинированного доступа пользователя и процесса к ресурсам.

3. Классификация объектов и субъектов доступа к ресурсам

3.3. Детальная классификация субъектов доступа

В качестве ресурсов, к которым должен разграничиваться доступ, должно выступать:

1. При автономном функционировании защищаемого объекта:
- логические диски (тома), каталоги, файлы данных;
- каталоги, не разделяемые ОС и приложениями (например, TEMP, «Корзина» и др.);
- каталоги с исполняемыми файлами, исполняемые файлы (обеспечение замкнутости программной среды);
- системный диск (где располагаются каталоги и файлы ОС);
- объекты, хранящие настройки ОС, приложений, системы защиты (для ОС Windows – реестр ОС);
- устройства;
- отчуждаемые внешние накопители (дискеты, CD-ROM диски и т.д.).

2. При функционировании защищаемого объекта в составе ЛВС помимо вышеуказанных должны дополнительно рассматриваться следующие ресурсы:
- разделяемые в сети файловые объекты;
- разделяемые в сети устройства;
- хосты;
- сетевые информационные технологии (сетевые приложения и службы).