Материалы к практическому занятию № 2 по дисциплине

Управление доступом к ресурсам автоматизированных систем

Задание:

1. Изучить вопросы Лекции № 2

1. Виды политик управления доступом
2. Утечка права доступа и нарушение безопасности КС
3. Модель нарушителя

2. Отметьте любым символом правильные ответы на следующие вопросы:

В КС доступ субъекта к сущности разрешается самим субъектом	
В КС доступ субъекта к сущности разрешается системой управления доступом	
В КС доступ субъекта к сущности разрешается системой разграничения доступа	
В КС доступ субъекта к сущности разрешается администратором системы	
Политика управления доступом и информационными потоками является составной частью политики безопасности КС	
Политика безопасности КС является составной частью политики управления доступом и информационными потоками	
Политика безопасности КС — совокупность правил, регулирующих управление доступом к ресурсам КС.	
Политика безопасности КС — совокупность правил, регулирующих управление ресурсами, их защиту и распределение в пределах КС	
Политика безопасности КС — совокупность правил, регулирующих распределение ресурсов в пределах КС	

Какие виды политик управления доступом существуют?

Дискреционная политика управления доступом	
Непрерывная политика управления доступом	
Вероятностная политика управления доступом	
Функциональная политика управления доступом	
Мандатная (полномочная) политика управления доступом	
Политика функционального управления доступом	
Политика ролевого управления доступом	
Политика безопасности информационных потоков	
Политика запрета информационных потоков	
Политика изолированной программной среды	
Политика открытой программной среды	

Какие требования к политикам управления доступом сформулированы неправильно?

Дискреционная политика управления доступом — политика, соответствующая следующим требованиям управления доступом в КС:	
• все сущности (в том числе субъекты) должны быть идентифицированы, т.е. каждой сущности должен быть присвоенуникальный идентификатор;	
• задана матрица доступов, каждая строка которой соответствует сущности КС, столбец — субъекту КС, ячейка содержит список прав доступа субъекта к сущности, представляющий собой подмножество множества прав доступа, реализованных в КС;	
• субъект обладает правом доступа к сущности КС в том, и только в том случае, когда в ячейке матрицы доступов, соответствующей субъекту и сущности, содержится данное право доступа.	
Мандатная политика управления доступом — политика, соответствующая следующим требованиям управления доступом в КС:	
• все сущности КС должны быть идентифицированы;	
• задана решетка уровней конфиденциальности информации;	
• каждой сущности КС присвоен уровень конфиденциальности, задающий установленные ограничения на доступ к данной сущности;	
• каждому субъекту системы присвоен уровень доступа, задающий уровень полномочий данного субъекта в КС;	
• субъект может получить доступ к сущности КС только в случае, когда уровень доступа субъекта позволяет предоставить ему данный доступ к сущности с заданным уровнем конфиденциальности, и реализация доступа не приведет к возникновению информационных потоков от сущностей с низким уровнем конфиденциальности к сущностям с высоким уровнем конфиденциальности.	
*Политика ролевого управления доступо*м — политика, соответствующая следующим требованиям управления доступом в КС:	
• все сущности должны быть идентифицированы;	
• задано множество ролей, каждой из которых ставится в соответствие некоторое множество прав доступа к сущностям	
• каждый субъект обладает одной из разрешенных (авторизованных) для данного субъекта ролью;	
• субъект обладает правом доступа к сущности КС в случае, когда субъект обладает ролью, которой соответствует множество прав доступа, содержащее	

данное право доступа к данной сущности.	

Политика безопасности информационных потоков основана на разделении всех сущностей КС на два непересекающихся множества: • множество сущностей-источников; • множество сущностей-приемников.	
Политика изолированной программной среды	
• Целью реализации политики ИПС является задание порядка безопасного взаимодействия объектов КС, обеспечивающего невозможность воздействия на систему защиты КС и модификации ее параметров или конфигурации, результатом которого могло бы стать изменение заданной для КС политики управления доступом.	
• Политика ИПС реализуется путем изоляции объектов КС друг от друга и путем контроля порождения новых субъектов таким образом, чтобы в системе могли активизироваться только субъекты из предопределенного списка. При этом должна контролироваться целостность сущностей КС, влияющих на функциональность активизируемых субъектов.	

Утечка права доступа и нарушение безопасности КС.

Утечкой права доступа называется переход КС в состояние, в котором субъект получает к сущности право доступа из множества запрещенных прав доступа субъектов к сущностям N_r.	
Нарушением безопасности КС называется ее переход в состояние, в котором либо получен запрещенный доступ из N_a, либо произошла утечка запрещенного права доступа из N_r, либо реализован запрещенный информационный поток из N_f.	