Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Барахов В.М.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»

Для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Модели безопасности компьютерных систем» / составитель: В.М. Барахов. - Ульяновск: УлГУ, 2019. Настоящие методические указания предназначены для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке к лекциям, семинарам, лабораторным и курсовым работам и к экзамену по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 2/19 от 19.03.2019).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

основная:

1. Девянин П.Н. Модели безопасности компьютерных систем. Учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия», 2005. – 144 с.

дополнительная:

1. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. – Р.: Феникс, 2008. – 173 с.
2. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.
3. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.– М.: Издательство Агентства «Яхтсмен», 1996. – 192с.
4. Документация по Astra Linux SE.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1 РАЗДЕЛ 1. ОСНОВЫ ФОРМАЛЬНОЙ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

ТЕМА 1. ОСНОВЫ ФОРМАЛЬНОЙ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

Основные вопросы:

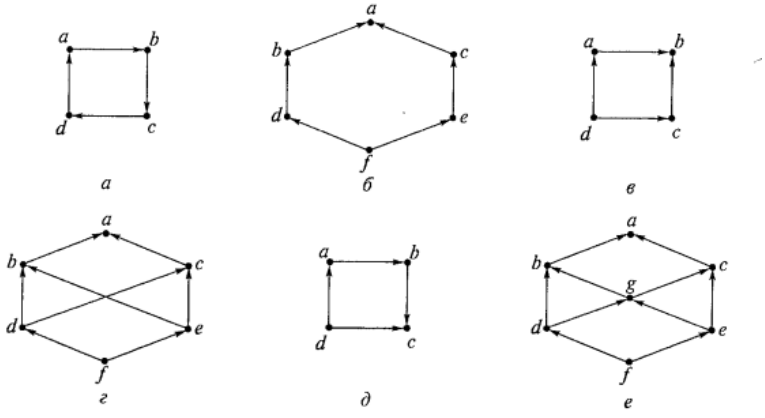
1. Основные понятия и определения.
2. Классификация угроз безопасности информации.
3. Основные виды политик безопасности.
4. Основные виды моделей безопасности.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 4-5.
Вопрос 2 изложен в учебном пособии [1] на с. 5-7.
Вопрос 3 изложен в учебном пособии [1] на с. 7-10.
Вопрос 4 изложен в учебном пособии [1] на с. 17.

Контрольные вопросы по теме 1:

1. В чем состоит важность основной аксиомы теории защиты информации?
2. Какие основные угрозы безопасности информации рассматриваются в теории защиты информации?
3. Приведите примеры наиболее распространенных в современных операционных системах и системах управления базами данных неблагоприятных информационных потоков по памяти и по времени.
4. Какие основные виды политик безопасности рассматриваются в теории защиты информации?
5. Задают ли решетку следующие графы?



Тесты для самостоятельной работы:

1. Основным видом доступа не является:

   a) read
   b) write
   c) delete
   d) execute

2. Выберите неправильное утверждение:

   a) В рамках субъект-сущностного подхода все вопросы безопасности информации в КС описываются доступам субъектов к сущностям.
   b) Все информационные потоки в КС порождены доступами субъектов к сущностям.
   c) Целостность информации — свойство информации, заключающееся в ее существовании в неискаженном виде.
   d) Информационный поток по памяти – информационный поток, при реализации которого фактор времени является существенным.

3. Какое из требований относится к дискреционной политике?

   a) задана решетка уровней конфиденциальности информации
   b) задана матрица доступов
   c) каждому субъекту системы присвоен уровень доступа, задающий уровень полномочий данного субъекта в КС
   d) каждый субъект обладает некоторым множеством разрешенных для данного субъекта ролей

2.2. РАЗДЕЛ 2. МОДЕЛИ СИСТЕМ С ДИСКРЕЦИОННЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

ТЕМА 2. МОДЕЛЬ МАТРИЦЫ ДОСТУПА ХАРРИСОНА – РУЗЗО – УЛЬМАНА

Основные вопросы:

1. Элементы модели ХРУ.
2. Анализ безопасности систем ХРУ.
3. Теорема о разрешимости задачи проверки безопасности монооперационных систем ХРУ.
4. Теорема о неразрешимости задачи проверки безопасности произвольной системы ХРУ.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 18-20.
Вопрос 2 изложен в учебном пособии [1] на с. 20-25.
Вопрос 3 изложен в учебном пособии [1] на с. 21.
Вопрос 4 изложен в учебном пособии [1] на с. 21-25.

Контрольные вопросы по теме 2:

1. Перечислите примитивные операторы модели ХРУ.
2. Что такое монооперационная система?

Тесты для самостоятельной работы:

1. Какой из операторов не является примитивным оператором модели ХРУ?

   a) «Создать» объект
   b) «Уничтожить» субъект
   c) «Прочитать» объект
   d) «Внести» право

2. Какой длины должна быть каждая последовательность команд при безопасном состоянии монооперационной системы?

   a) n
   b) n!
   c) n^2
   d) 2n

2.3. РАЗДЕЛ 2. МОДЕЛИ СИСТЕМ С ДИСКРЕЦИОННЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

ТЕМА 3. РАЗВИТИЕ МОДЕЛИ МАТРИЦЫ ДОСТУПОВ ХАРРИСОНА – РУЗЗО – УЛЬМАНА

Основные вопросы:

1. Формальное описание модели типизированной матрицы доступа (ТМД).
2. Каноническая форма модели МТМД (КФМТМД).
3. Модель ациклической монотонной ТМД (АМТМД).
4. Алгоритм построения развернутого состояния для системы АКФМТМД.
5. Теорема о разрешимости задачи проверки безопасности АМТМД.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 25-27.
Вопрос 2 изложен в учебном пособии [1] на с. 27-28.
Вопрос 3 изложен в учебном пособии [1] на с. 28-29.
Вопрос 4 изложен в учебном пособии [1] на с. 29.
Вопрос 5 изложен в учебном пособии [1] на с. 30-32.

Контрольные вопросы по теме 3:

1. Что такое модель монотонной типизированной матрицы доступов?
2. Что такое граф создания?
3. Когда система МТМД называется ациклической?
4. Какие системы называются тернарными?

Тесты для самостоятельной работы:

1. Какую сложность имеет алгоритм проверки безопасности систем АМТМД?

   a) Экспоненциальную
   b) Линейную
   c) Полиномиальную
   d) Асимптотическую

2. Каноническая форма модели МТМД – это:

a) Модель ТМД, в командах которой присутствуют немонотонные примитивные операторы вида «удалить»… и «уничтожить»…
b) Модель ТМД, в которой команды, содержащие примитивные операторы вида «создать»…, не содержат условий и примитивных операторов вида «внести»…
c) Модель ТМД, в которой команды, содержащие примитивные операторы вида «создать»…, содержат условия и примитивные операторы вида «внести»…
d) Модель ТМД, в командах которой отсутствуют немонотонные примитивные операторы вида «удалить»… и «уничтожить»…

2.4. РАЗДЕЛ 2. МОДЕЛИ СИСТЕМ С ДИСКРЕЦИОННЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

ТЕМА 4. КЛАССИЧЕСКАЯ МОДЕЛЬ РАСПРОСТРАНЕНИЯ ПРАВ ДОСТУПА TAKE – GRANT

Основные вопросы:

1. Формальное описание классической модели Take – Grant.
2. Санкционированное и несанкционированное получение прав доступа.
3. Граф доступов.
4. tg-связность вершин в графе доступа.
5. Понятия острова, моста и его начального и конечного пролетов в произвольном графе доступов.

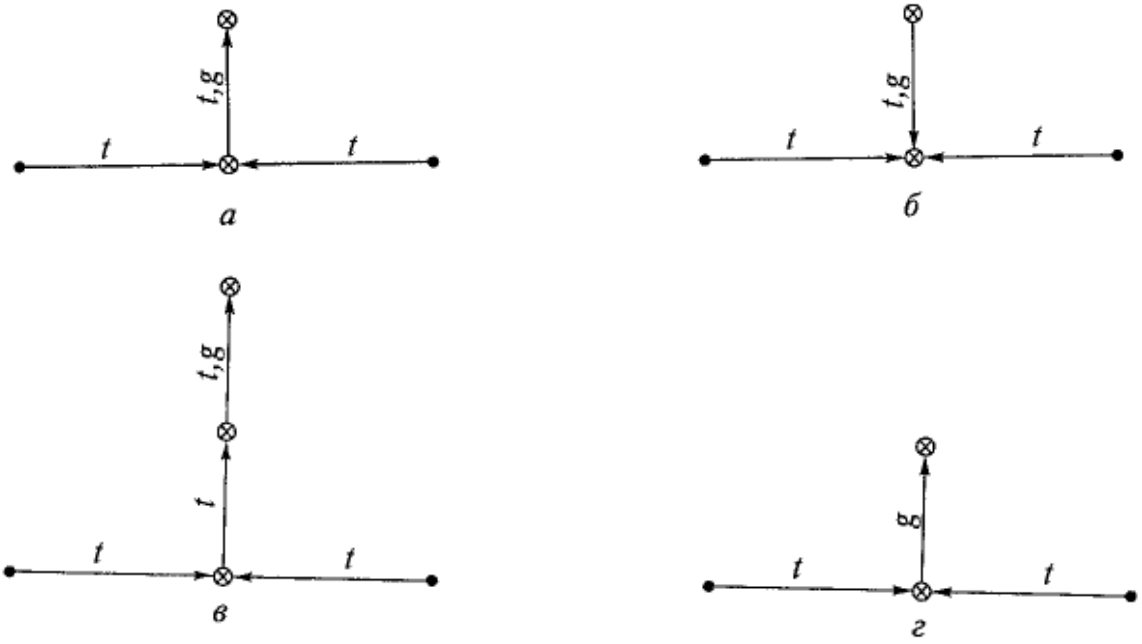
Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 32-33.
Вопрос 2 изложен в учебном пособии [1] на с. 34-35.
Вопрос 3 изложен в учебном пособии [1] на с. 35-36.
Вопрос 4 изложен в учебном пособии [1] на с. 36-48.
Вопрос 5 изложен в учебном пособии [1] на с. 38-42.

Контрольные вопросы по теме 4:

1. Как представить систему, построенную на основе модели Take – Grant, системой ТМД?
2. При каких условиях система Take – Grant может быть представлена системой АМТМД?

3. Являются ли мостами следующие графы?



Тесты для самостоятельной работы:

1. Классическая модель Take – Grant ориентирована на анализ путей распространения прав доступа в системах:

   a) изолированной программной среды
   b) мандатного разграничения доступа
   c) дискреционного разграничения доступа
   d) ролевого разграничения доступа

2. Какое из приведенных ниже правил не является основным де-юре правилом преобразования графа?

   a) delete()
   b) take()
   c) grant()
   d) create()

2.5. РАЗДЕЛ 2. МОДЕЛИ СИСТЕМ С ДИСКРЕЦИОННЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

ТЕМА 5. РАСШИРЕННАЯ МОДЕЛЬ РАСПРОСТРАНЕНИЯ ПРАВ ДОСТУПА TAKE – GRANT

Основные вопросы:

1. Направления развития модели Take – Grant.
2. Де-факто правила преобразования графов доступов и информационных потоков для расширенной модели Take – Grant.
3. Понятие замыкания графа доступов и информационных потоков расширенной модели Take – Grant и его разновидности.
4. Алгоритмы построения tg-замыкания, де-юре-замыкания, де-факто-замыкания.
5. Анализ путей распространения прав доступа и информационных потоков.
6. Подходы к определению стоимости пути в графе доступов и информационных потоков.

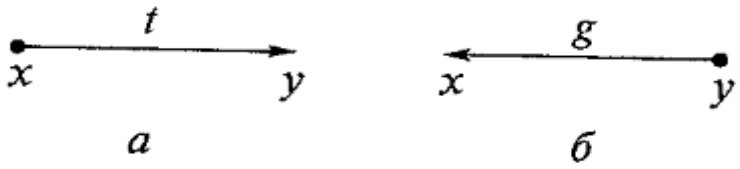
Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 43-44.
Вопрос 2 изложен в учебном пособии [1] на с. 44-47.
Вопрос 3 изложен в учебном пособии [1] на с. 47-48.
Вопрос 4 изложен в учебном пособии [1] на с. 48-50.
Вопрос 5 изложен в учебном пособии [1] на с. 50-51.
Вопрос 6 изложен в учебном пособии [1] на с. 51.

Контрольные вопросы по теме 5:

1. Как произвольную систему ТМД представить системой ХРУ?
2. Как по аналогии с определением безопасного начального состояния в модели ХРУ и с использованием определения предиката «возможен доступ» ( ) определить безопасное начальное состояние в модели Take – Grant?

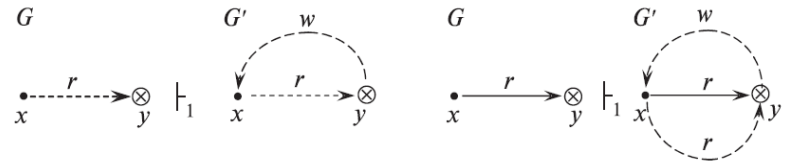
3. Как реализовать информационный поток на чтение от *x* к *y* и от *y* к *x* для систем со следующими графами доступов?



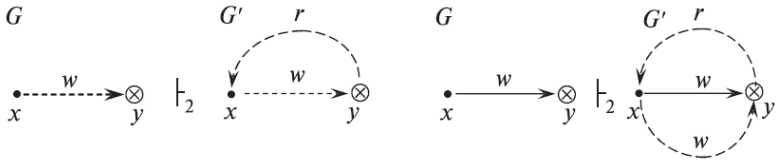
Тесты для самостоятельной работы:

1. На каком из рисунков показано применение первого де-факто правила?

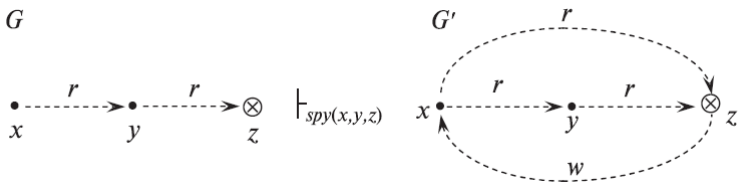
a)



b)



c)



2. Какой из этапов не входит в алгоритм построения замыкания графа доступов:

   a) Построение де-факто-замыкания
   b) Построение tg-замыкания.
   c) Построение де-юре-замыкания.
   d) Построение замыкания.

3. Из скольких шагов состоит алгоритм построения де-юре-замыкания?

   a) 3
   b) 5
   c) 4
   d) 7

2.6. РАЗДЕЛ 3. МОДЕЛИ СИСТЕМ С МАНДАТНЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

ТЕМА 6. КЛАССИЧЕСКАЯ МОДЕЛЬ БЕЛЛА – ЛАПАДУЛА

Основные вопросы:

1. Формальное описание классической модели Белла – ЛаПадула.
2. Основные запросы в классической модели Белла – ЛаПадула.
3. Теоремы об обладании системой *-свойством, ss-свойством и ds-свойством.
4. Базовая теорема безопасности.
5. Пример некорректного определения свойств безопасности.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 55-56.
Вопрос 2 изложен в учебном пособии [1] на с. 56.
Вопрос 3 изложен в учебном пособии [1] на с. 56-59.
Вопрос 4 изложен в учебном пособии [1] на с. 59-60.
Вопрос 5 изложен в учебном пособии [1] на с. 60-61.

Контрольные вопросы по теме 6:

1. Какие основные недостатки модели Белла – ЛаПадула?
2. Что такое система?
3. Докажите теорему БТБ.

Тесты для самостоятельной работы:

1. Выберите верное утверждение

   a) Состояние системы (b; m; f) называется безопасным, когда оно обладает *-свойством относительно S′, ss-свойством и ds-свойством.
   b) Система $\sum(Q;D;W; z_0)$ обладает ss-свойством, когда каждая ее реализация не обладает ss-свойством.
   c) В классической модели Белла–ЛаПадулы рассматриваются условия, при выполнении которых в КС возможно возникновение информационных потоков от объектов с большим уровнем конфиденциальности к объектам с меньшим уровнем конфиденциальности.

2.7. РАЗДЕЛ 3. МОДЕЛИ СИСТЕМ С МАНДАТНЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

ТЕМА 7. ИНТЕРПРЕТАЦИИ КЛАССИЧЕСКОЙ МОДЕЛИ БЕЛЛА – ЛАПАДУЛА

Основные вопросы:

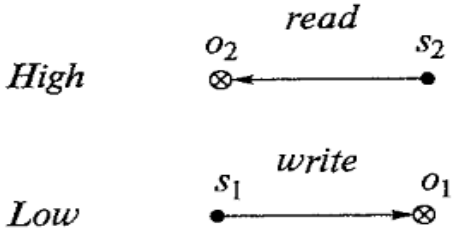
1. Политика low-watermark для модели Белла – ЛаПадула.
2. Безопасность переходов.
3. Теоремы об обладании системой *-свойством и ss-свойством.
4. Функции переходов и их использование в модели Белла – ЛаПадула.
5. Формальное описание модели мандатной политики целостности информации Биба.
6. Соответствие доступа требованиям политики low-watermark.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 61-63.
Вопрос 2 изложен в учебном пособии [1] на с. 63-64.
Вопрос 3 изложен в учебном пособии [1] на с. 64-65.
Вопрос 4 изложен в учебном пособии [1] на с. 65-66.
Вопрос 5 изложен в учебном пособии [1] на с. 66-67.
Вопрос 6 изложен в учебном пособии [1] на с. 67-68.

Контрольные вопросы по теме 7:

1. Как сформулировать теорему БТБ для модели мандатной политики целостности информации Биба?
2. Постройте пример системы Белла – ЛаПадула со следующими параметрами: S = {s_1, s_2}, O = {o_1, o_2}, R = {read, write}, (L, ≤) = {Low, High}, M – не используется, f_s (s_1) = f_o (o_1) = Low, f_s (s_2) = f_o (o_2) = High. Рассмотрите возможные варианты действия системы в состоянии, описываемом графом текущих доступов, по запросу субъекта s_2 на доступ на запись в объект o_1.



3. Переформулируйте определения ss-свойства и *-свойства функции переходов $T(s, q, (b, f)) = (b^*, f^*)$, включив в них определение безопасности функции переходов в смысле администрирования.

Тесты для самостоятельной работы:

1. Функции переходов и их использование в модели Белла – ЛаПадула это:

   a) Элементы модели, необходимые для реализации дискреционной политики безопасности.
   b) б) Модель контроля и управления доступом, основанная на мандатной модели управления доступом. В модели анализируется условия, при которых невозможно создание информационных потоков от субъектов с более высокого уровня доступа к субъектам более низкого уровня доступа.
   c) Безопасные начальные состояния, при которых система в целом будет безопасной;
   d) Дополнительные ограничения, используемые при определении свойств безопасности, в которых изменяется либо один элемент, либо множество текущих доступов, либо одно из значений одной из функций.

2. Какого вида доступа нет в модели Биба?

   a) modify
   b) invoke
   c) observe
   d) write

2.8. РАЗДЕЛ 3. МОДЕЛИ СИСТЕМ С МАНДАТНЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

ТЕМА 8. МОДЕЛЬ СИСТЕМ ВОЕННЫХ СООБЩЕНИЙ

Основные вопросы:

1. Основные определения, связанные с системой военных сообщений (СВС).
2. Неформальное описание модели СВС.
3. Формальное описание модели СВС.
4. Безопасная функция переходов
5. Базовая теорема безопасности для модели СВС.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 68-70.
Вопрос 2 изложен в учебном пособии [1] на с. 70-71.
Вопрос 3 изложен в учебном пособии [1] на с. 71-74.
Вопрос 4 изложен в учебном пособии [1] на с. 74-76.
Вопрос 5 изложен в учебном пособии [1] на с. 76-77.

Контрольные вопросы по теме 8:

1. Докажите теорему БТБ-СВС.
2. Каким образом десять неформальных свойств модели СВС реализуются в ее формальном описании?
3. Где в определениях безопасности модели СВС реализованы свойства безопасности (*-свойство, ss-свойство и ds-свойство) классической модели Белла – ЛаПадула?
4. Рассмотрите пример использования определения потенциальной модификации булевой сущности по ссылке r с источником булевой сущностью по ссылке y при запросе (u, i, s), реализующем функцию $V(r_{s*}) = V(r_s)$ *and* $V(y_s)$.

Тесты для самостоятельной работы:

1. Постулатом безопасности для СВС не является:

   a) Пользователь правильно определяет атрибут CCR контейнеров;
   b) Пользователь корректно направляет сообщение по адресатам и определяет множества доступа к созданным им самим сущностям;

c) Системный офицер безопасности корректно разрешает доступ пользователей к сущностям и назначает уровни конфиденциальности устройств и множества ролей;
d) Модель контроля и управления доступом, ориентированная на системы приема, передачи и обработки сообщений, реализующие мандатную политику безопасности.

2. Какое из свойств модели CBC не является неформальным:

a) Множество ролей пользователей;
b) Авторизация;
c) Иерархия уровней конфиденциальности;
d) Доступ по косвенной ссылке.

2.9. РАЗДЕЛ 4. МОДЕЛИ БЕЗПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ И ИЗОЛИРОВАННОЙ ПРОГРАММНОЙ СРЕДЫ

ТЕМА 9. АВТОМАТНАЯ МОДЕЛЬ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ

Основные вопросы:

1. Формальное описание автоматной модели безопасности информационных потоков.
2. Формальное описание программной модели контроля информационных потоков.
3. Контролируемый механизм защиты.
4. Вероятностная модель безопасности информационных потоков.
5. Информационная невыводимость.
6. Информационное невлияние.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 78-80.
Вопрос 2 изложен в учебном пособии [1] на с. 80-82.
Вопрос 3 изложен в учебном пособии [1] на с. 82-83.
Вопрос 4 изложен в учебном пособии [1] на с. 83-84.
Вопрос 5 изложен в учебном пособии [1] на с. 84.
Вопрос 6 изложен в учебном пособии [1] на с. 84-87.

Контрольные вопросы по теме 9:

1. Какой вид политики разграничения доступа используется в качестве основы автоматной модели безопасности информационных потоков7
2. Почему программная модель контроля информационных потоков может бать наиболее эффективно использована для систем защиты, реализованных в командных интерпретаторах?
3. Почему использование определения требований информационного невлияния (с учетом времени) позволяет обеспечить возможность функционирования в компьютерной системе монитора ссылок и системы аудита?

4. Постройте контролирующие механизмы защиты для следующих программ.

а)

```
Program1(x1, x2, x3)
{
    a = x1 − x2;
    if (x3 > 0)     y = a + x1;
    else            y = a + x2;
    y = y · x1;
}
```

б)

```
Program2(x1, x2, x3)
{
        a = x2 + x3;
        if (x1 = 0)     a = a + x3;
        else            a = a − x3;
        y = a − x2;
}
```

Тесты для самостоятельной работы:

1. Формальное описание автоматной модели безопасности информационных потоков это:

    a) Модель, в которой анализируются компьютерные системы, в которых реализована мандатная политика безопасности;
    b) Модель, в которой политика безопасности определяется через множество значений входных параметров;
    c) Модель, в которой предлагается механизм построения системы защиты, реализующей дискреционную политику безопасности для командных интерпретаторов;
    d) Модель, в которой система защиты представляется детерминированным автоматом, на вход которого поступает последовательность команд пользователей.
    e)

2. Вероятностная модель безопасности информационных потоков это:

    a) Модель, в которой требуется, чтобы низкоуровневая информация была независима от высокоуровневой;
    b) Модель, в которой анализируются компьютерные системы, в которых реализована мандатная политика безопасности;
    c) Модель, в которой задано динамическое количественное ограничение на обладание ролью.
    d) Модель, в которой возможна реализация мандатной политики безопасности, ориентированной на защиту от угрозы конфиденциальности информации.

2.10. РАЗДЕЛ 4. МОДЕЛИ БЕЗПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ И ИЗОЛИРОВАННОЙ ПРОГРАММНОЙ СРЕДЫ

ТЕМА 10. СУБЪЕКТНО – ОРИЕНТРИРОВАННАЯ МОДЕЛЬ ИЗОЛИРОВАННОЙ ПРОГРАММНОЙ СРЕДЫ

Основные вопросы:

1. Основные определения.
2. Объекты, функционально ассоциированные с субъектами.
3. Правила разграничения доступа субъектов к объектам.
4. Монитор безопасности объектов (МБО).
5. Достаточное условие гарантированного выполнения политики безопасности в компьютерной системе.
6. Изолированная программная среда (ИПС).
7. Состояние компьютерной системы.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 108-109.
Вопрос 2 изложен в учебном пособии [1] на с. 109-110.
Вопрос 3 изложен в учебном пособии [1] на с. 110-112.
Вопрос 4 изложен в учебном пособии [1] на с. 112-113.
Вопрос 5 изложен в учебном пособии [1] на с. 113-115.
Вопрос 6 изложен в учебном пособии [1] на с. 115-119.
Вопрос 7 изложен в учебном пособии [1] на с. 119-120.

Контрольные вопросы по теме 10:

1. Каковы основные функции МБО и МБС в ИПС, в чем их отличие друг от друга?
2. Почему для реализации ИПС необходимо требовать наличия в компьютерной системе контроля порождения субъектов?
3. В чем отличие структуры ядра безопасности в классических моделях безопасности компьютерных систем от структуры ядра безопасности в субъектно-ориентированной модели ИПС?
4. Рассмотрите на примере реальных компьютерных систем пути реализации в них требований субъектно-ориентированной модели ИПС при ступенчатой загрузке.

Тесты для самостоятельной работы:

1. Субъектно-ориентированная модель ИПС это:

   a) Модель, в которой политика безопасности определяется через множество значений входных параметров;
   b) Модель, в которой требования политики безопасности в большинстве случаев определяется с использованием математических моделей;
   c) Модель, в которой основное внимание уделяется определению порядка безопасного взаимодействия субъектов системы;
   d) Модель, в которой анализируются компьютерные системы, в которых реализована мандатная политика безопасности.

2. Выберите неверное утверждение:

   a) Монитор безопасности субъектов (МБС) —МПС, который разрешает порождение субъектов только для фиксированного множества пар активизирующих субъектов и объектов источников.
   b) КС называется замкнутой по порождению субъектов (обладает замкнутой программной средой), когда в ней действует МБС.
   c) Монитор безопасности объектов (МБО) — МО, который разрешает любые потоки.
   d) Монитор порождения субъектов (МПС) — субъект, активизирующийся при любом порождении субъектов.

2.11. РАЗДЕЛ 5. МОДЕЛИ СИСТЕМ С РОЛЕВЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

ТЕМА 11. БАЗОВАЯ МОДЕЛЬ РОЛЕВОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

Основные вопросы:

1. Понятие ролевого разграничения доступа (РРД).
2. Формальное описание базовой модели РРД.
3. Иерархия ролей.
4. Механизм ограничений в базовой модели РРД.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 88.
Вопрос 2 изложен в учебном пособии [1] на с. 88-89.
Вопрос 3 изложен в учебном пособии [1] на с. 89-90.
Вопрос 4 изложен в учебном пособии [1] на с. 90-91.

Контрольные вопросы по теме 11:

1. Перечислите основные элементы базовой модели РРД.
2. Что подразумевается под иерархией ролей в базовой модели РРД?

Тесты для самостоятельной работы:

1. Ролевое разграничение доступа это:

   a) Определение порядка безопасного взаимодействия субъектов системы, обеспечивающего невозможность воздействия на систему защиты и модификацию ее параметров или конфигурации, результатом которых могло бы стать изменение реализуемой системы защиты политики разграничения доступа;
   b) Модель - дающая ответ на вопрос о возможности получения прав доступа субъектом системы на объект в состоянии, описываемом графом доступов;
   c) Модель, в которой анализируются компьютерные системы, в которых реализована мандатная политика безопасности;
   d) Развитие политики дискреционного разграничения доступа; при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли.

2.12. РАЗДЕЛ 5. МОДЕЛИ СИСТЕМ С РОЛЕВЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

ТЕМА 12. МОДЕЛЬ АДМИНИСТРИРОВАНИЯ РОЛЕВОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

Основные вопросы:

1. Формальное описание модели администрирования РРД.
2. Администрирование множеств авторизованных ролей пользователей.
3. Администрирование множеств прав доступа, которыми обладают роли.
4. Администрирование иерархии ролей.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 92-93.
Вопрос 2 изложен в учебном пособии [1] на с. 93-97.
Вопрос 3 изложен в учебном пособии [1] на с. 97-98.
Вопрос 4 изложен в учебном пособии [1] на с. 98-101.

Контрольные вопросы по теме 12:

1. Какие основные проблемы определения правил изменения иерархии ролей рассматриваются в модели администрирования РРД?

Тесты для самостоятельной работы:

1. Что не относится к задачам администрирования ролевого управления доступом?

   a) администрирование множеств правил доступа
   b) администрирование множеств авторизованных ролей пользователей
   c) администрирование множеств прав доступа, которыми обладают роли
   d) администрирование иерархии ролей

2. Выберите ошибочное суждение:

   a) Роли-возможности — роли, которые обладают только заданными в соответствующей возможности правами доступа.
   b) Роли-группы — роли, на которые могут быть авторизованы одновременно несколько пользователей соответствующей группы.

c) Роли-объединения — роли, которые обладают возможностями, правами доступа и на которые могут быть авторизованы группы пользователей и отдельные пользователи.

2.13. РАЗДЕЛ 5. МОДЕЛИ СИСТЕМ С РОЛЕВЫМ РАЗГРАНИЧЕНИЕМ ДОСТУПА

ТЕМА 13. МОДЕЛЬ МАНДАТНОГО РОЛЕВОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

Основные вопросы:

1. Защита от угрозы конфиденциальности информации.
2. Защита от угроз конфиденциальности и целостности информации.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 101-103.
Вопрос 2 изложен в учебном пособии [1] на с. 103-107.

Контрольные вопросы по теме 13:

1. Какого вида ограничения, описанные в базовой модели РРД, могут быть использованы при определении требований либерального и строгого мандатного разграничения доступа?
2. Докажите, что при соответствии модели РРД требованиям либерального или строгого мандатного разграничения доступа для каждого доступа (o, write) существует единственная роль x_write, такая, что (o, write) ∈ PA(x_write) (здесь x = c(o)).
3. Каким образом в определениях либерального или строгого мандатного разграничения доступа модели РРД реализованы ss-свойство и *-свойство, определенные в классической модели Бела – ЛаПадула?

Тесты для самостоятельной работы:

1. К мандатному разграничению доступом не относится:

    a) Обеспечение выполнения требований пометки субъектов и объектов
    b) Определение порядка функционирования доверенных субъектов компьютерной системы
    c) Основным элементом является матрица доступов
    d) Обеспечение безопасности информационных потоков

2.14. РАЗДЕЛ 6. ПРИМЕНЕНИЕ И ДАЛЬНЕЙШЕЕ РАЗВИТИЕ МОДЕЛЕЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

ТЕМА 14. ПРОБЛЕМА АДЕКВАТНОСТИ РЕАЛИЗАЦИИ МОДЕЛИ БЕЗОПАСНОСТИ В РЕАЛЬНОЙ КОМПЬЮТЕРНОЙ СИСТЕМЕ

Основные вопросы:

1. Общая постановка задачи построения системы защиты.
2. Гомоморфизм компьютерной системы и ее математической модели безопасности.
3. Проблемы реализации дискреционной политики безопасности.
4. Проблемы реализации мандатной политики безопасности.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 121-122.
Вопрос 2 изложен в учебном пособии [1] на с. 122-123.
Вопрос 3 изложен в учебном пособии [1] на с. 123-124.
Вопрос 4 изложен в учебном пособии [1] на с. 125-128.

Контрольные вопросы по теме 14:

1. В чем состоит основная проблема реализации системы защиты в произвольной компьютерной системе?
2. Возможна ли реализация атаки с использованием программных закладок вида «троянский конь» в системах с мандатным разграничением доступа?

Тесты для самостоятельной работы:

1. Какая проблема является наиболее существенной при реализации реальных систем дискреционной политики?

    a) Проблема отсутствия в большинстве математических моделей четких правил разграничения доступа
    b) Проблема обеспечения безопасности информационных потоков
    c) Проблема обеспечения выполнения требований пометки субъектов и объектов
    d) Проблема обхода неблагоприятных информационных потоков с использованием локальных и логических переменных

2. Что необходимо сделать для предотвращения неблагоприятных информационных потоков через локальные или логические переменные при написании программ?

   a) Отрывать все файлы в конце выполнения программы
   b) Производить обработку информации из открытых файлов, используя только логические переменные
   c) Производить обработку информации из открытых файлов только во внешних процедурах, использующих только локальные переменные
   d) Открывать все файлы, необходимые для работы программы в начале ее выполнения

2.15. РАЗДЕЛ 6. ПРИМЕНЕНИЕ И ДАЛЬНЕЙШЕЕ РАЗВИТИЕ МОДЕЛЕЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

ТЕМА 15. БАЗОВОЕ АДМИНИСТРИРОВАНИЕ НА ПРИМЕРЕ АДМИНИСТРИРОВАНИЯ ОС СЕМЕЙСТВА ASTRA LINUX.

Основные вопросы:

1. Обоснование политики безопасного администрирования.
2. Математическая модель политики безопасного администрирования.
3. Требования к настройке, конфигурированию и администрированию ОС и их обоснование.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 128-129.
Вопрос 2 изложен в учебном пособии [1] на с. 129-136.
Вопрос 3 изложен в учебном пособии [1] на с. 136-137.

Контрольные вопросы по теме 15:

1. Каким образом мандатная политика целостности Биба была использована для обоснования политики безопасного администрирования компьютерных систем?
2. Перечислите все требования к настройке, конфигурированию и администрированию ОС.

Тесты для самостоятельной работы:

1. Какая угроза не рассматривается в политике безопасного администрирования?

   a) Угроза получения пользователем всех привилегий на данном компьютере
   b) Угроза захвата привилегий одного пользователя другим при размещении личных ресурсов на компьютере
   c) Угроза запрета администратору домена осуществлять удаленное обращение к рабочим станциям и входить на них локально