МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Факультет вычислительной техники

Кафедра Информационной безопасности

ОЦЕНОЧНЫЕ СРЕДСТВА

дисциплины

**«****Модели безопасности компьютерных систем» (****Б 1.Б.11)**

Специальность – 10.05.01 «Компьютерная безопасность»

Специализация N 8 "Информационная безопасность объектов информатизации на базе компьютерных систем"

Уровень подготовки специалитет

 Форма обучения - очная

Срок обучения — 5 лет 6 месяцев

Рязань 2019 г.**Общие положения**

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур, оцениваемых ресурсов в дистанционных учебных курсах), предназначенных для оценки качества освоения обучающимися дисциплины «Модели безопасности компьютерных систем» как части основной образовательной программы.

## Назначение

Цель – оценить соответствие знаний, умений и уровня приобретённых компетенций, обучающихся целям и требованиям основной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний, обучающихся проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся: на занятиях; по результатам выполнения контрольных работ; по результатам выполнения обучающимися типовых расчётов; по результатам проверки качества конспектов лекций и иных материалов. При оценивании (определении) результатов освоения дисциплины применяется традиционная шкала оценивания («отлично», «хорошо», «удовлетворительно», «неудовлетворительно», «зачет», незачет»).

Текущая аттестация студентов проводится на основании результатов выполнения ими типовых расчётов (ТР) и контрольных работ (КР).

По итогам изучения разделов дисциплины «Основы теории надёжности», обучающиеся в конце каждого учебного семестра, проходят промежуточную аттестации. Форма проведения аттестации – экзамен в устной, письменной формах или тест: электронный билет, формируемый случайным способом. Экзаменационные билеты и перечни вопросов, задач, примеров, выносимых на промежуточную аттестацию, составляются с учётом содержания тем учебной дисциплины и подписываются заведующим кафедрой.

В экзаменационный билет или вариант теста включаются два теоретических вопроса и до четырёх практических задач по темам дисциплины (Протокол заседания кафедры Информационной безопасности №10 от 26 апреля 2017г.).

## **Паспорт оценочных материалов по дисциплине**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Контролируемые модули (темы) дисциплины (результаты по разделам) | Код контролируемой компетенции (или её части) | Вид, метод, форма оценочного мероприятия |
| **Семестр 6** |
| 1. | Введение в теоретический подход к обеспечению информационной безопасности.  | ОПК–4, ПК-4, ОПК-9 | Опрос, зачет |
| 2. | Математические основы построения моделей безопасности.  | ОПК–4, ПК-4, ОПК-9 | Опрос, зачет |
| 3. | Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU).  | ОПК–4, ПК-4, ОПК-9 | Опрос, зачет |
| 4. | Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД).  | ОПК–4, ПК-4, ОПК-9 | Опрос, зачет |
| 5. | Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant.  | ОПК–4, ПК-4, ОПК-9 | Опрос, зачет |
| 6. | Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы.  | ОПК–4, ПК-4, ОПК-9 | Опрос, зачет |
| 7. | Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений.  | ОПК–4, ПК-4, ОПК-9 | Опрос, зачет |
| 8. | Модели компьютерных систем с ролевым управлением.  | ОПК–4, ПК-4, ОПК-9 | Опрос, зачет |
| 9. | Модели безопасности информационных потоков и изолированной программной среды.  | ОПК–4, ПК-4, ОПК-9 | Опрос, зачет |
| 10. | Формальные модели безопасности компьютерных систем. | ОПК–4, ПК-4, ОПК-9 | Опрос, зачет |

## Критерии оценивания компетенций (результатов)

1) Уровень усвоения материала, предусмотренного программой.

2) Умение анализировать материал, устанавливать причинно-следственные связи.

3) Качество ответа на вопросы: полнота, аргументированность, убежденность, логичность.

4) Содержательная сторона и качество материалов, приведенных в отчетах студента по типовым расчетам, практическим занятиям.

5) Использование дополнительной литературы при подготовке ответов.

Уровень освоения сформированности знаний, умений и навыков по дисциплине оценивается в форме бальной отметки. Критерии оценивания промежуточной аттестации представлены в таблице.

|  |  |  |
| --- | --- | --- |
| **Четырёхбальная шкала оценивания** | **Двухбалльная шкала оценивания** | **Критерии оценивания** |
| **«отлично»** | **«зачтено»** | **студент должен**: продемонстрировать глубокое и прочное усвоение знаний материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; правильно формулировать определения; уметь сделать выводы по излагаемому материалу; безупречно ответить не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины; продемонстрировать умение правильно выполнять практические задания, предусмотренные программой;  |
| **«хорошо»** | **«зачтено»** | **студент должен:** продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; уметь сделать достаточно обоснованные выводы по излагаемому материалу; ответить на все вопросы билета; продемонстрировать умение правильно выполнять практические задания, предусмотренные программой, при этом возможно допустить непринципиальные ошибки. |
| **«удовлетворительно»** | **«зачтено»** | **студент должен:** продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины; уметь устранить допущенные погрешности в ответе на теоретические вопросы и/или при выполнении практических заданий под руководством преподавателя, либо (при неправильном выполнении практического задания) по указанию преподавателя выполнить другие практические задания того же раздела дисциплины. |
| **«неудовлетворительно»** | **«незачтено»** | **ставится в случае:** незнания значительной части программного материала; не владения понятийным аппаратом дисциплины; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы по излагаемому материалу. Оценка «неудовлетворительно» («незачтено») выставляется также, если студент после начала экзамена отказался его сдавать или нарушил правила сдачи экзамена (списывал, подсказывал, обманом пытался получить более высокую оценку и т.д.).  |

## Фонд оценочных средств дисциплины включает

– задачи практических занятий;

– оценочные средства промежуточной аттестации;

### Задачи для практических занятий

В ходе практических занятий происходит решение задач, представленных в сборниках задач для практических занятий и самостоятельной работы, типичными являются.

*Тема «Математические основы построения моделей безопасности»*

1.1. Нарисуйте граф, соответствующий решетке многоуровневой безопасности (X x L, ≤), для решетки (L, ≤) = {Low, Middle, High) и (X, ≤) — решетки подмножеств множества U = {Political, Military}. 1.2. Задают ли решетку графы на рисунке?

*Тема «Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU)»*

2.1. Для команды C(qi0, ai0) = (qi1, ai1, l) машины Тьюринга выпишите две представляющие ее команды модели ХРУ.

2.2. Докажите, что для общего случая систем ХРУ не существует алгоритма проверки возможности утечки права доступа r для заданной пары субъект s и объект о.

2.3. Представьте произвольную систему ТМД системой ХРУ.

2.4. Постройте графы создания для систем МТМД со следующими наборами команд.

а) command a1(x: α, у: β, z: β)

«создать» субъект х с типом α;

end;

command а2(х: α, у: γ, z: β,s: δ)

«создать» объект у с типом γ;

«создать» субъект s с типом δ;

end;

command a3(x: ε, у: δ, z: β, s: γ, o: δ)

«создать» субъект о с типом δ;

«создать» объект х с типом ε;

end.

б) command a1(x: α, у: β, z: γ)

«создать» субъект у с типом β;

«создать» субъект х с типом α;

end;

command а2(х: β, у: δ, z: δ)

«создать» субъект z с типом δ;

end;

command a3(x: ε, у: α, z: δ)

«создать» объект x с типом ε;

end.

*Тема «Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД)»*

3.1. Истинен ли предикат can\_share(α, х, у, G0) для графа доступов G0 на рисунке?

3.2. Истинен ли предикат can\_write(x, у, G0) для графа доступов G0 на рисунке? Выбор последовательности объектов oi, ..., om не является однозначным.

3.3. Как реализовать информационный поток на запись от субъекта х к субъекту у и от субъекта у к субъекту х для систем с графами доступов на рисунке далее.

3.4. Постройте tg-замыкания графов доступов на рисунке далее.

*Тема «Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant»*

4.1. Постройте пример, иллюстрирующий порядок применения правила flow(x, у, у`, z) базовой ДП-модели.

4.2. В рамках базовой ДП-модели рассмотрим правило преобразования графов доступов spy(x, y, z) со следующим условием применения: х,уϵS, zϵЕ, x≠z, {(x, y, readr), (x, y, readr)}⊂ R, и результатом применения: S'=S, E`=E, R`=R, A`=A, F`=F U {(z, x, writem)}. Выразите правило spy(x, y, z) с применением правил базовой ДП-модели.

4.3. Сформулируйте и обоснуйте достаточные условия, при выполнении которых в рамках базовой ДП-модели предикат can\_share{α, x, y,G0, Ls) является ложным, т.е. невозможна утечка права доступа (x, у, α).

4.4. Сформулируйте и обоснуйте необходимые и достаточные условия истинности предикатов can\_write\_memory(x, у, G0, LS) и can\_write\_time(x, у, G0, LS) для начального состояния G0 = (S0, Е0, R0UA0UF0, H0) системы Σ(G\*, OP, G0), в которомА0=F0= Ø.

*Тема «Формальные модели безопасности компьютерных систем»*

5.1. В рамках ФАС ДП-модели постройте последовательность правил преобразования состояний, позволяющих субъекту х получить право доступа владения ownr к единственному доверенному субъекту у.

5.2. В рамках ФПАС ДП-модели докажите следующее утверждение. Пусть G0=(S0, Е0, R0UA0UF0, H0) — состояние системы Σ (G\*, OP) и недоверенный субъект хϵNs∩S0, субъект уϵS0, где х≠у. Пусть истинен предикат directly\_can\_share\_own(x, у, G0, Ls), тогда является истинным предикат can\_share\_own(x, у, G0, Ls).

*Тема «Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы»*

6.1. Опишите состояние системы Белла-ЛаПадулы со следующими параметрами S={s1,s2}, O={o1,o2}, R={read, write}, (L, ≤)={Low, High}, M – не используется, fs(s1)=fo(o1)=Low, fs(s2)=fo(o2)=High. Рассмотрите возможные варианты действий системы в состоянии, описываемом графом текущих доступов, изображённому на рисунке, по запросу субъекта s2 на доступ на запись к объекту о1. Подсчитайте количество различных состояний системы для следующих случаев: когда в системе не требуется выполнение свойств безопасности; когда в системе требуется выполнение только ss-свойства; когда в системе требуется выполнение ss-свойства и \*-свойства.

6.2. 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.

*Тема «Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений»*

7.1. Пусть, а, b, с, d — компьютеры, α, β, γ — сетевые информационные каналы, определяемые как совокупность команд сетевых интерфейсов. Опишите КС, представленную на рис. 5.6, с использованием семи требований информационного невлияния автоматной модели безопасности информационных потоков.

7.2. Постройте контролирующие механизмы защиты для следующих программ. Являются ли они максимальными

а)

Program1 (x1, x2 , x3)

{

a = x1 - x2;

if (x3 > 0) у = а + x1;

else у = а + x2 ;

у = y · x1;

}

б)

Program2 (x1, x2 , x3)

{

a = x2+x3;

if (х1  == 0) а = а + х3;

else а = а – х3;

у = а – х2;

}

7.3. Постройте примеры ДП-моделей систем, реализующих отождествление порожденных субъектов или политику строгого мандатного управления доступом.

*Тема «Модели компьютерных систем с ролевым управлением»*

8.1. Докажите, что при соответствии модели ролевого управления доступом требованиям либерального или строгого мандатного управления доступом для каждого доступа (o, write) ∈ P существует единственная роль x\_write такая, что (o, write) ∈ PA(x\_write) (здесь x = c(o)).

8.2. Постройте графы иерархии ролей для модели мандатного ролевого управления доступом для решеток уровней конфиденциальности (L, ≤) = {LS, MS, HS} и уровней целостности (LI,≤) = {LI, MI, HI}.

8.3. Постройте пример системы ∑(G\*, OP) с состоянием G0 = {PA0, user0, roles0,А0,F0,Не0), в котором для недоверенного пользователя х ∈ NU, прав доступа к сущности (е, а), (е, ownr) ∈ Р0, где a ≠ ownr, истинны предикаты directly\_can\_share((e,ownr),х,G0) и can\_share((e,ownr),х,G0), а предикаты directly\_can\_share((e,a),x,G0) и can\_share((e, a), x, G0) являются ложными.

### Оценочные средства промежуточной аттестации

Фонд оценочных средств промежуточной аттестации, проводимой в форме экзамена, зачета или теста, включает

1. типовые теоретические вопросы;
2. дополнительные вопросы;
3. типовые практические задачи.

Оценочные средства приведены ниже для семестра обучения. Разрешается и иная формулировка вопроса или примера, без изменения его смысла или содержания, например, дробление, изменение условий или иное.

**Примеры типовых теоретических вопросов к экзамену**

1. Определение политики безопасности.
2. Взаимосвязь задач защиты информации.
3. Субъектно-объектная модель системы.
4. Значение и роль стандартов информационной безопасности.
5. Формальные модели управления доступом.
6. Модель дискреционного доступа Харрисона-Руззо- Ульмана.
7. Модель ТМД (типизированная матрица доступа).
8. Модель Take-Grant (TG).
9. Базовая модель ролевого управления (RBAC).
10. Модель Бела-ЛаПадулы (БЛП).
11. Модель ролевого администрирования.
12. Ролевая модель Forсe-Field.
13. Модель Биба.
14. Модель Кларка-Вильсона.
15. Модель Брюэра-Нэша («Китайская стена»).
16. Модель Гогена-Мезигера (GM).
17. Модель Лендвера-МакЛина (СВС).
18. Объединение моделей БЛП и Биба.
19. Объединение ролевой модели и модели Биба.
20. Модель выявления безопасности Деннинга.
21. Модель Graham-Denning.
22. Политика безопасности Диона.
23. Политика описания информационных потоков.
24. Направления развития мандатных и ролевых моделей.
25. Модели изолированной мандатной среды.
26. Базовая ДП-модель.
27. Семейство дискреционных ДП-моделей.
28. Семейство мандатных ДП-моделей.
29. Методика построения моделей безопасности информации.

|  |  |  |
| --- | --- | --- |
| Составил:к.т.н., доцент каф. ИБ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | (Копейкин Ю.А.) |
| Заведующий кафедрой ИБ,к.т.н, доцент | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | (Пржегорлинский В.Н.) |