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

|  |  |
| --- | --- |
| СОГЛАСОВАНОДекан факультетавычислительной техники\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.А. Перепелкин«\_\_\_\_»\_\_\_\_\_\_\_\_\_20\_\_\_ г. | УТВЕРЖДАЮПроректор РОПиМД\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В.Корячко «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_\_ г  |
| Руководитель ОПОП\_\_\_\_\_\_\_\_\_\_\_\_ В.Н. Пржегорлинский«\_\_\_»\_\_\_\_\_\_\_\_\_20\_\_\_\_ г. |  |

**РАБОЧАЯ ПРОГРАММА**

дисциплины

**«****Модели безопасности компьютерных систем» (****Б1.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.ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования

 по специальности 10.05.01 Компьютерная безопасность (уровень специалитета)

утвержденного Приказом Минобрнауки России от 01.12.2016 г. № 1512

Разработчики

Доцент кафедры Информационной безопасности

(должность, кафедра)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Копейкин Ю.А.

 (подпись) (Ф.И.О.)

Программа рассмотрена и одобрена на заседании кафедры

«\_\_\_» \_\_\_\_\_\_\_\_ 20\_\_ г., протокол № \_\_\_\_\_

Заведующий кафедрой

 \_\_Информационной безопасности\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 ( кафедра)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Пржегорлинский В.Н.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (Ф.И.О.)

**1.** **Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательных программ специалитета**

Рабочая программа по дисциплине «Модели безопасности компьютерных **систем**» является составной частью основной профессиональной образовательной программы по направлению подготовки специалистов 10.05.01 Компьютерная безопасность (уровень специалитета), разработанной в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.05.01 Компьютерная безопасность (уровень специалитета), утвержденным приказом Минобрнауки России от 01.12.2016 г. № 1512

## *Целю изучения* дисциплины «Модели безопасности компьютерных систем» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации; обучение общим принципам построения моделей безопасности и политик безопасности, основным методам исследования корректности систем защиты, методологии обследования и проектирования систем защиты.

## *Задачи дисциплины:*

* изложение теоретических основ компьютерной безопасности;
* описание моделей безопасности информационных систем;
* описание моделей доступа в информационных системах;
* обучение методологии обследования и проектирования систем защиты;
* обучение навыкам настройки основных компонентов систем защиты и применения технологий защиты.

## Перечень планируемых результатов обучения по дисциплине

|  |  |  |
| --- | --- | --- |
| **Компетенции** | **Содержание****компетенций** | **Перечень планируемых результатов обучения по дисциплине** |
| ОПК-4 | Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над межди-сциплинарными и инновационными проектами. | Знать: методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами. Уметь: применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами. Владеть: методами научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами  |
| ОПК-9 | Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации. | Знать: формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом безопасности информации. Уметь: разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом безопасности информации. Владеть: способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом безопасности информации.  |
| ПК-4 | Способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем. | Знать:методы формального описания моделей угроз и злоумышленника; основные способы формального описания и анализа политик безопасности, построения математических моделей безопасности компьютерных систем; Уметь:разрабатыватьмодели угроз и злоумышленника; описывать и анализировать политику информационной безопасности автоматизированных систем, разрабатывать математические модели безопасности компьютерных систем; Владеть:навыками разработки математических моделей угроз и злоумышленника; навыками анализа политик безопасности автоматизированных информационных систем.  |

**2. Место дисциплины в структуре ОПОП подготовки бакалавров**

Дисциплина «Модели безопасности компьютерных систем» является обязательной и относится к базовой части блока №1 (Б1.Б.11) основной профессиональной образовательной программы подготовки специалистов направления 10.05.01 Компьютерная безопасность (уровень специалитета) специализации «Информационная безопасность объектов информатизации на базе компьютерных систем».

Дисциплина изучается по очной форме обучения на 3 курсе в 6 семестре.

*Пререквизиты дисциплины*:

* «Основы информационной безопасности»;
* «Информатика»;
* «Теория информации»;
* «Аппаратные средства вычислительной техники»;
* «Защита в операционных системах»;
* «Криптографические методы защиты информации»;
* «Математическая логика и теория алгоритмов»;
* «Основы построения защищенных баз данных»;
* «Основы построения защищенных компьютерных сетей».

Для освоения дисциплины обучающийся должен:

**знать:**

* классификацию современных компьютерных систем;
* основные понятия математической логики и теории алгоритмов;
* основные понятия и методы дискретной математики;
* источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
* защитные механизмы и средства обеспечения безопасности операционных систем.

***уметь***:

* формализовать поставленную задачу;
* осуществлять программную реализацию алгоритма;
* проводить оценку сложности алгоритмов;
* составлять модель угроз для информационной системы;
* реализовывать основные методы обеспечения информационной безопасности информационных систем;

*Постреквизиты дисциплины*:

* прохождении производственной и преддипломной практик;
* выполнении выпускной квалификационной работы.

**3. объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Общая трудоемкость дисциплины составляет 5 зачетных единиц (ЗЕ), 180 часов.

Форма обучения – очная

|  |  |
| --- | --- |
| **Вид учебной работы** | **Всего часов** |
| **Очная форма** |
| Общая трудоемкость дисциплины, в том числе: | 180 |
| 1. Контактная работа обучающихся с преподавателем (всего), в том числе: | 48 |
| Лекции  | 24 |
| Лабораторные работы | - |
| Практические занятия | 24 |
| 2. Самостоятельная работа обучающихся (всего), в том числе: | 132 |
| Контроль  | 36 |
| курсовая работа | - |
| курсовой проект | - |
| иные виды самостоятельной работы | 96 |
| 3. Форма контроля  | Экзамен |

# 4. содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

## 4.1 *Содержание дисциплины, структурированное по темам (разделам)*

|  |  |
| --- | --- |
| **Раздел дисциплины** | **Содержание** |
| 1. Введение в теоретический подход к обеспечению информационной безопасности.  | 1. Основные понятия защиты информации (субъекты, объекты, доступ, граф доступов, информационные потоки). Постановка задачи построения защищенной автоматизированной системы (АС). Ценность информации.
 |
| 2. Математические основы построения моделей безопасности.  | 1. Применение теории графов и теории автоматов для обеспечения информационной безопасности информационных систем. Понятие автомата, графа, математической решетки. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы. Проблема адекватности реализации модели безопасности в реальной компьютерной системе.
 |
| 3. Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU).  | 1. Определение дискреционного контроля доступа. Принципы построения матрицы доступов. Контроль над процессом передачи прав доступа в системе. Модель системы безопасности Харрисона-Руззо-Ульмана (HRU). Основные положения модели. Теорема об алгоритмической неразрешимости задачи проверки безопасности произвольной системы HRU
 |
| 1. 4. Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД).
 | Модель типизированной матрицы доступов. Основные положения модели. Теорема о существовании алгоритма проверки безопасности ациклических систем монотонных ТМД. |
| 5. Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant.  | Модель распространения прав доступа Take-Grant. Теоремы о передаче прав в графе доступов, состоящем из субъектов, и произвольном графе доступов. Расширенная модель Take-Grant и ее применение для анализа информационных потоков в АС. |
| 6. Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы.  | Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели. Базовая теорема безопасности (BST). Политика low-watermark в модели Белла-ЛаПадулы. |
| 7. Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений.  | Применение модели Биба для реализации мандатной политики целостности. Применение модели систем военных сообщений для систем приема, передачи и обработки почтовых сообщений, реализующих мандатную политику безопасности. Шесть теоретических принципов политики контроля целостности. Соответствие правил модели Кларка-Вилсона принципам политики целостности. |
| 8. Модели компьютерных систем с ролевым управлением.  | Понятие ролевого управления доступом. Базовая модель ролевого управления доступом. Понятие администрирования ролевого управления доступом. Администрирование иерархии ролей. Понятие мандатного ролевого управления доступом. Требования либерального мандатного управления доступом. |
| 9. Модели безопасности информационных потоков и изолированной программной среды.  | Автоматная модель безопасности информационных потоков. Вероятностная модель безопасности информационных потоков. Информационное невлияние. Информационное невлияние с учетом фактора времени. Монитор безопасности объектов. Монитор безопасности субъектов. Теоремы о достаточных условиях гарантированного выполнения политики безопасности в компьютерных системах. Базовая теорема изолированной программной среды. |
| 10. Формальные модели безопасности компьютерных систем. | Взаимосвязь положений и основные направления развития формальных моделей безопасности компьютерных систем Взаимосвязь положений классических формальных моделей безопасности КС. Критический анализ классических моделей. Проблема адекватности реализации модели безопасности в реальной КС.Семейство моделей безопасности логического управления доступом и информационными потоками (ДП-моделей).Развитие формальных моделей. Обзор семейства формальных моделей управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным или ролевым управлением доступом. Доверенные и недоверенные субъекты. Анализ информационных потоков по памяти или по времени. Функционально или параметрически ассоциированные с субъектами сущности. |

1. **4.2. *Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах).***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Раздел дисциплины** | **Общая трудоемкость, всего часов** | **Контактная работа обуча-ющихся с преподавателем** | **Самостоятельная работа обучающихся** |
| всего | лекции | семинары, практические занятия | лабораторные работы |
| 1. | Введение в теоретический подход к обеспечению информационной безопасности.  | **11** | 3 | 1 | 2 |  | 8 |
| 2. | Математические основы построения моделей безопасности.  | **11** | 3 | 1 | 2 |  | 10 |
| 3. | Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU).  | **17** | 7 | 3 | 4 |  | 10 |
| 4. | 1. Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД).
 | **15** | 5 | 3 | 2 |  | 10 |
| 5. | Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant.  | **17** | 7 | 2 | 4 |  | 10 |
| 6. | Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы.  | **14** | 4 | 2 | 2 |  | 10 |
| 7 | Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений.  | **14** | 4 | 2 | 2 |  | 10 |
| 8 | Модели компьютерных систем с ролевым управлением.  | **15** | 5 | 3 | 2 |  | 10 |
| 9 | Модели безопасности информационных потоков и изолированной программной среды.  | **13** | 5 | 3 | 2 |  | 8 |
| 10 | Формальные модели безопасности компьютерных систем. | **16** | 6 | 4 | 2 |  | 10 |
| 11 | Контроль (экзамен) | **36** |  |  |  |  | 36 |
|  | **Всего по дисциплине:** | **180** | **48** | **24** | **24** | **-** | **132 (96+36)** |

**Виды практических, лабораторных и самостоятельных работ**

| **№ п/п** | **Тема** | **Вид работы** | **Наименование и содержание работы** | **Трудо-емкость, часов** |
| --- | --- | --- | --- | --- |
| 1 | Введение в теоретический подход к обеспечению информационной безопасности.  | Практическая работа | Построение модели безопасности информационной системы с помощью теории автоматов и теории графов. | 2 |
| Самостоятельная работа обучающегося | Изучение конспекта лекцийПодготовка и выполнение ПЗ | 8 |
| 2 | Математические основы построения моделей безопасности. | Практическая работа | Построение модели безопасности информационной системы с помощью вероятностного подхода. | 2 |
| Самостоятельная работа обучающегося | Изучение конспекта лекцийПодготовка и выполнение ПЗ | 10 |
| 3 | 1. Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU).
 | Практическая работа | 1) Реализация дискреционной модели безопасности (модель Харрисона-Руззо-Ульмана).2). Решение задач на модель ХРУ. | 4 |
| Самостоятельная работа обучающегося | Изучение конспекта лекцийПодготовка и выполнение ПЗ | 10 |
| 4 | 1. МоМодели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД).
 | Практическая работа | Реализация дискреционной модели безопасности с типизированной матрицей доступа (ТМД) | 2 |
| Самостоятельная работа обучающегося | Изучение конспекта лекцийПодготовка и выполнение ПЗ | 10 |
| 5 | Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant. | Практическая работа | 1) Реализация дискреционной модели доступа (модель Take-Grant). 2) Решение задач на модели доступа Take-Grant. | 4 |
| Самостоятельная работа обучающегося | Изучение конспекта лекцийПодготовка и выполнение ПЗ | 10 |
| 6 | Модели компьютерных систем с мандатным управлением. Модель Белла-ЛаПадулы. | Практическая работа | 1) Реализация мандатной модели доступа (модель Белла-ЛаПадулы). Решение задач на модель Белла-ЛаПадулы).  | 2 |
| Самостоятельная работа обучающегося | Изучение конспекта лекцийПодготовка и выполнение ПЗ | 10 |
| 7 |  Модели компьютерных систем с мандатным управлением. Модель Биба. Модель систем военных сообщений. | Практическая работа | 1) Реализация модели Биба. Реализация модели систем военных сообщений. Сравнительный анализ модели Биба и модели систем военных сообщений. | 2 |
| Самостоятельная работа обучающегося | Изучение конспекта лекцийПодготовка и выполнение ПЗ | 10 |
| 8 | Модели компьютерных систем с ролевым управлением.  | Практическая работа | 1) Реализация ролевой модели разграничения прав доступа (RBAC). Реализация администрирования иерархии ролей. Реализация атрибутивной модели доступа. Сравнительный анализ атрибутивной и ролевой моделей доступа. | 2 |
| Самостоятельная работа обучающегося | Изучение конспекта лекцийПодготовка и выполнение ПЗ | 10 |
| 9 | Модели безопасности информационных потоков и изолированной программной среды.  | Практическая работа | 1) Реализация моделей безопасности информационных потоков и изолированной программной среды. Сравнительный анализ модели безопасности информационных потоков и изолированной программной среды. | 2 |
| Самостоятельная работа обучающегося | Изучение конспекта лекцийПодготовка и выполнение ПЗ | 8 |
| 10 | Формальные модели безопасности компьютерных систем. | Практическая работа | Развитие формальных моделей. Формальные модели управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным или ролевым управлением доступом. | 2 |
| Самостоятельная работа обучающегося | Изучение конспекта лекцийПодготовка и выполнение ПЗ | 10 |
| 12 | Экзамен | Самостоятельная работа обучающегося | Изучение конспекта лекций.Подготовка к экзамену | 36 |

1. **5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине**
2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и ин-формационными потоками. Учебное пособие для вузов. М.: Горячая линия -Телеком, 2011. –320 с.
3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - 452 с.
4. Кабанов А.С., Лось А.Б., Першаков А.С. Теоретические основы компьютер-ной безопасности, М: РИО МИЭМ.-2012.-245 с.
5. Расторгуев С.П. Основы информационной безопасности: учеб. пособие для студ. высших учебных заведений. - М.: Издательский центр «Академия», 2007.
6. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. - М.: Книжный мир, 2009. - 352 с.
7. Прикладная дискретная математика. - Томск: ООО «Издательство научно-технической литературы».

**6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине**

Фонд оценочных средств приведен в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «*Модели безопасности компьютерных систем*»).

1. 7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

## Основная литература

1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2011. - 320 с.
2. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - 452 с.
3. Кабанов А.С., Лось А.Б., Першаков А.С. Теоретические основы компьютер-ной безопасности, М: РИО МИЭМ.-2012.-245 с.
4. Башлы, П.Н. Информационная безопасность и защита информации: Учебник [Электронный ресурс] / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – М.: РИОР, 2013. – 222 с. – Режим доступа: [http://znanium.com/bookread.php?book=405000](http://znanium.com/bookread.php?book=405000%20) (дата обращения 01.02.2015);
5. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие [электронный ресурс] / В.Ф. Шаньгин. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. – 592 с. – Режим доступа: [http://znanium.com/bookread.php?book=402686](http://znanium.com/bookread.php?book=402686%20) (дата обращения 01.02.2015).

## Дополнительная литература

1. Расторгуев С.П. Основы информационной безопасности: учеб. пособие для студ. высших учебных заведений. - М.: Издательский центр «Академия», 2007. - 192 с.
2. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. - М.: Гелиос АРВ, 2006. - 528 с.
3. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. - М.: Книжный мир, 2009. - 352 с.
4. Bishop M. Computer Security: art and science. - ISBN 0-201-44099-7, 2002. - 1084 p.
5. Прикладная дискретная математика. - Томск: ООО «Издательство научно-технической литературы».
6. Проблемы информационной безопасности. Компьютерные системы. - СПб.: Издательство Политехнического университета.
7. Пакин А.И. Информационная безопасность информационных систем управления предприятием [Электронный ресурс]: учебное пособие по части курса / А.И. Пакин. — Электрон. текстовые данные. — М.: Московская государственная академия водного транспорта, 2009. — 41 c. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/46462.html>
8. Александровская Л.Н. Безопасность и надежность технических систем [Электронный ресурс]: учебное пособие / Л.Н. Александровская, И.З. Аронов, В.И. Круглов. — Электрон. текстовые данные. — М.: Логос, 2008. — 376 c. — 978-5-98704-115-5. — Режим доступа: <http://www.iprbookshop.ru/9055.html>.

**8. Ресурсы информационно–телекоммуникационной сети Интернет, базы данных, информационно-справочные и поисковые системы**

1. Сайт кафедры Информационная безопасность РГРТУ: <http://www.rsreu.ru/faculties/fvt/kafedri/ib>

*Общедоступные Интернет-ресурсы*

1. сайт Экспонента: <http://old.exponenta.ru/>
2. Единое окно доступа к образовательным ресурсам: <http://window.edu.ru/>
3. Интернет Университет Информационных Технологий: <http://www.intuit.ru/>
4. Сайт GeoGebra: <https://www.geogebra.org/>
5. ФСБ России [Электронный ресурс]. –Режим доступа: <http://fsb.ru> (дата обращения 01.02.2015);
6. 2. ФСТЭК России [Электронный ресурс]. –Режим доступа: <http://fstec.ru> (дата обращения 01.02.2015).

*Обучающимся предоставлена возможность индивидуального доступа к следующим электронно-библиотечным системам.*

1. Электронная библиотека РГРТУ, режим доступа с любого компьютера без пароля. – URL: <http://elib.rsreu.ru/>
2. Электронно-библиотечная система «IPRbooks», режим доступа – с любого компьютера РГРТУ без пароля, из сети интернет по паролю. – URL: <https://iprbookshop.ru/>

9. Методические указания для обучающихся по освоению дисциплины

Дисциплина «Модели безопасности компьютерных систем» предусматривает лекции, практические занятия в соответствии с учебным планом. В семестре изучение тем дисциплины завершается промежуточной аттестацией.

Успешное изучение курса требует посещения лекций, активной работы на практических занятиях самостоятельных занятий, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой.

## Работа с лекциями

При изучении дисциплины очень полезно самостоятельно изучать материал, который еще не прочитан на лекции и не применялся на практическом занятии. Тогда лекция будет гораздо понятнее.

Однако легче при изучении курса следовать изложению материала на лекции. Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий.

После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня.

Лекцию необходимо прочитать, заполнить пропуски, расшифровать и уточнить некоторые сокращения, дополнить некоторые недописанные примеры. Особое внимание следует уделить содержанию понятий.

Все новые понятия должны выделяться в тексте, чтобы их легко можно было отыскать и запомнить.

Лекционный материал является важным, но не единственным для изучения учебной дисциплины. Его необходимо дополнить материалом из рекомендуемой литературы по теме.

Если обучающемуся самостоятельно не удалось разобраться в материале, необходимо сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

При подготовке к следующей лекции, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции.

## Подготовка к практическому занятию и лабораторной работе

Подготовка состоит в теоретической подготовке (изучение конспекта лекций и дополнительной литературы) и выполнении практических заданий (решение задач, ответы на вопросы и т.д.). Во время самостоятельных занятий студенты выполняют задания, выданные им на предыдущем практическом занятии, готовятся к контрольным работам, выполняют задания типовых расчётов.

## Указания в рамках подготовки к промежуточной аттестации

Промежуточная аттестация проходит в виде экзамена (зачета) или теста, к которому допускаются обучающиеся, выполнившие и сдавшие (защитившие) все предусмотренные учебной программой контрольные мероприятия: контрольные работы и типовые расчёты. Промежуточная аттестация может проводиться в следующих формах:

- Устная форма экзамена (зачета) предусматривает устные ответы на вопросы билета к экзамену. При этом, для уточнения оценки, студенту могут быть заданы дополнительные вопросы.

- Письменная форма экзамена (зачета) предусматривает проверку письменных ответов на вопросы билета к экзамену.

- Тестовая форма (электронный билет, формируемый случайным способом) предусматривает выполнение студентом заданий теста в письменной форме (теоретических или практических), которые проверяются преподавателем или автоматически.

При подготовке к промежуточной аттестации в дополнение к изучению конспектов лекций, учебных пособий, слайдов и другого раздаточного материала, предусмотренного рабочей программой дисциплины, необходимо пользоваться учебной литературой, рекомендованной к настоящей рабочей программе. При подготовке к промежуточной аттестации следует изучить теорию: определения всех понятий и подходы к оцениванию до состояния понимания материала и самостоятельно решить по нескольку типовых задач из каждой темы, из задачника или дистанционного учебного курса. При решении задач всегда необходимо уметь качественно интерпретировать итог решения. Обязательно присутствовать на консультации перед промежуточной аттестации.

## **Указания в рамках самостоятельной работы студентов**

Самостоятельная работа студентов по дисциплине играет важную роль в ходе всего учебного процесса. Методические материалы, рекомендации и дистанционные учебные курсы для обеспечения самостоятельной работы студентов готовятся преподавателем и выдаются студентам в виде раздаточных материалов или оформляются в виде электронного ресурса, используемого в рамках системы дистанционного обучения ФГБОУ ВО «РГРТУ».

Для реализации компетентностного подхода используются как традиционные формы и методы обучения, так и интерактивные формы, направленные на формирование у студентов навыков коллективной работы и умения анализировать различные материалы.

Для полноценного закрепления материала, представляемого на лекционных занятиях, требуется решение примеров и задач на практических занятиях, а также регулярное выполнение самостоятельной работы, которые необходимы для проверки теоретических знаний и формирования практических навыков.

# **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине**

В рамках реализации образовательной программы при проведении занятий используются следующие информационные технологии:

- удаленные инфррмационные коммуникации между студентами и преподавателем, ведущим лекционные и практические занятия, посредством электронно-образовательной среды, позволяющие осуществлять оперативный контроль графика выполнения и содержания контрольных заданий, решениеорганизационных вопросов, удаленное консультирование;

- поиск актуальной информации для выполнения самостоятельной работы и контрольных заданий;

При проведении практических занятий и самостоятельной работы студентов используется программное обеспечение:

1) лицензионная копия операционной системы Windows версии не ниже ХР;

2) свободно распространяемая программа интерактивной математики GeoGebra;

3) свободно распространяемая система дистанционного обучения Moodle;

4) браузер (Firefox, Google, Opera);

5) дистанционные курсы по темам дисциплины, разработанные в системе дистанционного обучения преподавателями кафедры Moodle.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для освоении дисциплины необходимы:

* + 1. для проведения лекционных занятий необходима аудитория с достаточным количеством посадочных мест, соответствующая необходимым противопожарным нормам и санитарно-гигиеническим требованиям;
		2. для проведения лекционных занятий требуется комплект технических средств обучения в составе:
* Переносной компьютер.
* Проектор (разрешение не менее 1280х1024).
	+ 1. для практических занятий используются учебные аудитории РГРТУ, оборудованные доской для представления учебного материала.

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.05.01 «Компьютерная безопасность»— специалитет, форма обучения — очная.

Программу составил

к.т.н., доц. кафедры ИБ Копейкин Ю.А.

#### Программа рассмотрена и одобрена на заседании

кафедры ИБ (протокол № от .2019 г.)

Зав. кафедрой ИБ

к.т.н., доц. Пржегорлинский В.Н.

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.) |