Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Первый проректор –
проректор по учебной работе
__________Н.Г. Кузнецов
«01» июня 2018г.

Рабочая программа дисциплины
Модели разграничения доступа

по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Квалификация
Бакалавр

Ростов-на-Дону
2018 г.

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
Недель	17,3			
Вид занятий	УП	РПД	УП	РПД
Лекции	36	36	36	36
Лабораторные	36	36	36	36
В том числе инт.	36	36	36	36
Итого ауд.	72	72	72	72
Контактная работа	72	72	72	72
Сам. работа	36	36	36	36
Часы на контроль	36	36	36	36
Итого	144	144	144	144

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 "Информационная безопасность" (уровень бакалавриата) (приказ Минобрнауки России от 01.12.2016г. №1515)

Рабочая программа составлена по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Учебный план утвержден учёным советом вуза от 27.03.2018 протокол № 10.

Программу составил(и): ктн, доцент, Скляров А.В. _____ 10.05.18

Зав. кафедрой: д.э.н. Тищенко Е.Н. _____ 11.05.18

Методическим советом направления: к.ф-м.н, доцент, Карасев Д.Н. _____ 15.05.18

Отделом образовательных программ и планирования учебного процесса Торопова Т.В. _____ 30.05.18

Проректором по учебно-методической работе Джуха В.М. _____ 31.05.18

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2019-2020 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой д.э.н. Тищенко Е.Н. _____

Программу составил(и): ктн, доцент, Скляров А.В. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2020-2021 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой д.э.н. Тищенко Е.Н. _____

Программу составил(и): ктн, доцент, Скляров А.В. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой: д.э.н. Тищенко Е.Н. _____

Программу составил(и): ктн, доцент, Скляров А.В. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой: д.э.н. Тищенко Е.Н. _____

Программу составил(и): ктн, доцент, Скляров А.В. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Изучить теоретические основы информационной безопасности (ИБ) и методологические нормы системного обеспечения защиты информационных процессов в компьютерных системах.
1.2	Задачи дисциплины:
1.3	-раскрытие понятийного аппарата в области ИБ и ЗИ в компьютерных системах;
1.4	-раскрытие содержательных базовых положений;
1.5	-раскрытие современной доктрины ИБ;
1.6	-определение целей и принципов ЗИ в компьютерных системах;
1.7	-установление факторов, влияющих на ЗИ;
1.8	-установление угроз информации в компьютерных системах;
1.9	-раскрытие направлений, видов, методов и особенностей деятельности злоумышленников в компьютерной сети и при наличии изолированного компьютера;
1.10	-раскрытие назначения, сущности и структуры системы ЗИ в компьютерных системах, системных вопросов защиты программ и данных;
1.11	-определение требований к программной и программно-аппаратной реализации средств ЗИ в компьютерных системах и к защите АСУ от несанкционированного доступа (НСД).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Для успешного освоения дисциплины студент должен иметь базовую подготовку по математике и информатике
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Моделирование процессов и систем защиты информации
2.2.2	Основы управления информационной безопасностью
2.2.3	Преддипломная практика

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Знать:
Физические основы программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Уметь:
Осуществлять научно обоснованный выбор программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Владеть:
Методиками научно обоснованного вы-бора программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.
ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты
Знать:
Принципы построения и функционирования подсистемы информационной безопасности объекта защиты
Уметь:
Осуществлять научно обоснованный выбор способов администрирования подсистемы информационной безопасности объекта защиты
Владеть:
Методиками научно обоснованного выбора способов администрирования подсистемы информационной безопасности объекта защиты.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)							
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Интер акт.**	**Примечание**
	Раздел 1. Исходные положения теории компьютерной безопасности						

1.1	Математические основы моделей безопасности. Основные понятия Элементы теории автоматов Элементы теории графов /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
1.2	Содержание и основные понятия компьютерной безопасности История развития теории и практики обеспечения компьютерной безопасности Содержание и структура понятия компьютерной безопасности Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности /Лек/	6	2	ПК-1	Л1.1	1	
1.3	Политика безопасности в компьютерных системах Понятие политики безопасности информации в компьютерных системах Субъектно-объектная модель компьютерной системы в механизмах и процессах коллективного доступа к информационным ресурсам /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
1.4	Элементы теории защиты информации Математические основы моделей безопасности. Основные понятия Элементы теории автоматов Элементы теории графов /Лаб/	6	4	ПК-1 ПК-3	Л1.1 Л2.1	2	
1.5	Математические основы моделей безопасности. Содержание и структура понятия компьютерной безопасности Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности /Лаб/	6	4	ПК-1 ПК-3	Л1.1 Л2.1	2	
1.6	Основные составляющие моделей безопасности Математические основы моделей безопасности. Содержание и структура понятия компьютерной безопасности Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности /Ср/	6	6	ПК-1 ПК-3	Л1.1 Л2.1	0	
	Раздел 2. Модели безопасности компьютерных систем						
2.1	Модели безопасности на основе дискреционной политики. Общая характеристика политики доступа Модель ХРУ Основные расширения модели /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	Модели безопасности на основе дискреционной политики
2.2	Модели безопасности на основе мандатной политики Общая характеристика политики мандатного доступа Модель Белла-ЛаПадулы Основные расширения модели Белла-ЛаПадулы /Лек/	6	2	ПК-3	Л1.1 Л2.1	1	Общая характеристика политики мандатного доступа Модель Белла-ЛаПадулы Основные

2.3	Модели безопасности на основе ролевой политики Общая характеристика моделей разграничения доступа на основе функционально- ролевых отношений /Лек/	6	2	ПК-3	Л1.1 Л2.1	1	Общая характеристика моделей разграничения доступа на
2.4	Исследование модели матрицы доступа ХРУ. Модели безопасности на основе дискреционной политики. Общая характеристика политики доступа Модель ХРУ Основные расширения модели /Лаб/	6	4	ПК-1	Л1.1 Л2.1	2	
2.5	Исследование модели распространения прав доступа. Модели безопасности на основе ролевой политики Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений /Лаб/	6	4	ПК-1 ПК-3	Л1.1 Л2.1	2	
2.6	Элементы теории защиты информацииМодели безопасности на основе ролевой политики Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений /Ср/	6	6	ПК-1 ПК-3	Л1.1 Л2.1	0	
	Раздел 3. Нейтрализация скрытых каналов утечки информации на основе технологий "представлений" и "разрешенных процедур"						
3.1	Нейтрализация каналов утечки информации на основе технологий "представлений" и "разрешенных процедур" Каналы утечки Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
3.2	Понятие моделей обеспечения целостности данных /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
3.3	Общая характеристика моделей и технологий обеспечения целостности данныхОбщая характеристика политики мандатного доступа Модель Белла-ЛаПадулы Основные расширения модели Белла-ЛаПадулы /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
3.4	Исследование модели Белла-Ла Падула. Общая характеристика политики мандатного доступа Модель Белла-ЛаПадулы Основные расширения модели Белла-ЛаПадулы /Лаб/	6	4	ПК-1 ПК-3	Л1.1 Л2.1	2	
3.5	Исследование модели систем военных сообщений.Общая характеристика политики мандатного доступа Модель Белла-ЛаПадулы Основные расширения модели Белла-ЛаПадулы /Лаб/	6	4	ПК-1 ПК-3	Л1.1 Л2.1	2	
3.6	Математические основы моделей безопасности Общая характеристика политики мандатного доступа Модель Белла-ЛаПадулы Основные расширения модели Белла-ЛаПадулы /Ср/	6	6	ПК-1 ПК-3	Л1.1 Л2.1	0	

	Раздел 4. Технологии обеспечения целостности данных						
4.1	Дискреционная модель Кларка- Вильсона Общая характеристика моделей и технологий обеспечения целостности данныхОбщая характеристика политики мандатного доступа Модель КВ Основные расширения модели /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
4.2	Мандатная модель Кена Биба Общая характеристика моделей и технологий обеспечения целостности данныхОбщая характеристика политики доступа Модель Основные расширения модели /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
4.3	Технологии параллельного выполнения транзакций в клиент-серверных системахОбщая характеристика моделей и технологий обеспечения целостности данныхОбщая характеристика политики мандатного доступа Модель Основные расширения модели /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
4.4	Исследование модели ролевого разграничения доступа. /Лаб/	6	4	ПК-1 ПК-3	Л1.1 Л2.1	2	
4.5	Модели систем дискриминационного разграничения доступа /Ср/	6	6	ПК-1 ПК-3	Л1.1 Л2.1	0	
	Раздел 5. Политика и модели безопасности в распределенных компьютерных системах						
5.1	Общая характеристика проблем безопасности в распределенных компьютерных системах /Лек/	6	2	ПК-1 ПК-3	Л1.1 Л2.1	1	
5.2	Модели распределенных систем в процессах разграничения доступа /Лек/	6	2	ПК-3	Л1.1 Л2.1	1	
5.3	Разграничение доступа к информации в распределенных компьютерных системах на основе зональной модели /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
5.4	Исследование модели ролевого разграничения доступа /Лаб/	6	4	ПК-3	Л1.1 Л2.1	2	
5.5	Базовая модель ролевого разграничения доступа /Ср/	6	6	ПК-3	Л1.1 Л2.1	0	
	Раздел 6. Методы анализа и оценки защищенности компьютерных систем						
6.1	Теоретико-графовые модели комплексной оценки защищенности /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
6.2	Теоретико-графовая модель системы индивидуально-групповых назначений доступа к иерархически организованным объектам /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	
6.3	Пространственно-векторная модель и характеристики системы рабочих групп пользователей /Лек/	6	2	ПК-1	Л1.1 Л2.1	1	

6.4	Исследование модели администрирования ролевого разграничения доступа Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений /Лаб/	6	4	ПК-1 ПК-3	Л1.1 Л2.1	2	
6.5	Модель администрирования ролевого разграничения доступа Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений /Ср/	6	6	ПК-1	Л1.1 Л2.1	0	
6.6	экзамен по темам дисциплины /Экзамен/	6	36	ПК-1 ПК-3	Л1.1 Л2.1 Э1 Э2	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

ВОПРОСЫ

1. Место ИБ в системе национальной безопасности;
2. Основные принципы обеспечения ИБ;
3. Классификация угроз ИБ;
4. Состав и краткая характеристика внутренних и внешних источников угроз ИБ;
5. Сущность и понятие информационной безопасности (ИБ);
6. Характеристика основных составляющих ИБ;
7. Значение ИБ для субъектов информационных отношений
8. Состав и краткая характеристика основных угроз доступности;
9. Состав и краткая характеристика основных угроз целостности;
10. Состав и краткая характеристика основных угроз конфиденциальности;
11. Классификация категорий хакеров и их целей;
12. Состав и краткая характеристика организационно□коммуникативных средств НСД;
13. Состав и краткая характеристика технических средств НСД;
14. Состав и краткая характеристика программных средств НСД;
15. Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;
16. Классификация сетевых атак;
17. ; Основные составляющие моделей безопасности
18. Элементы теории защиты информации
19. Математические основы моделей безопасности
20. Модели систем дискриминационного разграничения доступа
21. Модель матрицы доступа ХРУ
22. Модель распространения прав доступа
23. Модели систем мандатного разграничения доступа
24. Модель Белла-Ла Падула
25. Модель систем военных сообщений
26. Модели систем ролевого разграничения доступа
27. Понятие ролевого разграничения доступа
28. Базовая модель ролевого разграничения доступа
29. Модель администрирования ролевого разграничения доступа
30. Основные принципы архитектурной безопасности и их краткая характеристика;

5.2. Фонд оценочных средств для проведения текущего контроля

Структура и содержание фонда оценочных средств представлены в Приложении 1 к рабочей программе дисциплины

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Мельников Д. А.	Информационная безопасность открытых систем: учеб. для студентов, обучающихся по напр. "Приклад. информатика"	М.: Флинта, 2013	20

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А.	Информационная безопасность и защита информации: учеб. пособие для студентов вузов, обучающихся по спец. "Информ. системы и технологии"	М.: Академия, 2012	20

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"	
Э1	Цифровые образовательные ресурсы: http://www.cor.home-edu.ru
Э2	Федеральный центр информационно-образовательных ресурсов (ФЦИОР): http://fcior.edu.ru
6.3. Перечень программного обеспечения	
6.3.1	Браузеры: Internet Explorer, Mozilla Firefox, Google Chrome;
6.3.2	Справочно-правовая система «Консультант +»,
6.3.3	Microsoft Word, 1C, OpenSSH, ClamAV,
6.3.4	ClamWin, Eclipse, Free Pascal, Tor, I2P;
6.4 Перечень информационных справочных систем	
6.4.1	
6.4.2	Компьютерная справочно-правовая система «Гарант»,
6.4.3	НТЦ «Система»

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Лаборатория физики
7.2	Лаборатория управления информационной безопасностью
7.3	Лаборатория электротехники, электроники и схемотехники
7.4	Учебный серверный центр
7.5	Лаборатория технической защиты информации
7.6	Лабораторпия систем и сетей передачи информации
7.7	Лаборатория программно-аппаратных средств обеспечения информационной безопасности
7.8	Лаборатория защищенных информационных систем

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
Методические указания по усвоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины

Приложение 1
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры Информационных
технологий и защиты информации
Протокол №10 от «11» мая 2018 г.
Зав.кафедрой _____ *Тищенко Е.Н.*

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Б1.В.ОД.10 «Модели разграничения доступа»
(наименование дисциплины)
Направление подготовки

10.03.01 «Информационная безопасность»

Уровень образования
бакалавриат

Составитель _____ Скляров А.В., доцент, к.т.н.
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Оглавление

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

1.1 Перечень компетенций с указанием этапов их формирования представлен в п. 3. «Требования к результатам освоения дисциплины» рабочей программы дисциплины.

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

2.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации			
З: Физические основы программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа
У: Пользоваться программными, программно-аппаратными (в том числе криптографическими) и техническими средств защиты информации	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа

В: Методами установки, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты			
З: основы администрирования подсистемы информационной безопасности объекта защиты	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа
У: Пользоваться программными, программно-аппаратными средствами администрирования подсистемы информационной безопасности объекта защиты	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа

В: Методами установки, настройки и обслуживания подсистемы информационной безопасности объекта защиты	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	ЛР – лабораторная работа

2.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале.

- 84-100 баллов (оценка «отлично») - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- 67-83 баллов (оценка «хорошо») - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- 50-66 баллов (оценка удовлетворительно) - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- 0-49 баллов (оценка неудовлетворительно) - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы».

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

«Ростовский государственный экономический университет (РИНХ)»

Кафедра Информационных технологий и защиты информации
(наименование кафедры)

Вопросы к экзамену

по дисциплине «Модели разграничения доступа»
(наименование дисциплины)

1. Основные составляющие моделей безопасности
2. Элементы теории защиты информации
3. Математические основы моделей безопасности
4. Модели систем дискриминационного разграничения доступа
5. Модель матрицы доступа ХРУ
6. Модель распространения прав доступа
7. Модели систем мандатного разграничения доступа
8. Модель Белла-Ла Падула
9. Модель систем военных сообщений
10. Модели систем ролевого разграничения доступа
11. Понятие ролевого разграничения доступа
12. Базовая модель ролевого разграничения доступа
13. Модель администрирования ролевого разграничения доступа
14. Основные принципы архитектурной безопасности и их краткая характеристика;
15. Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;
16. Основные функции централизованного управления рисками и администрирования системы безопасности;
17. Основные функции защиты управления приложениями;
18. Основные функции защиты системы сетей;
19. Основные функции защиты конечных пользователей;
20. Классификация средств защиты программного обеспечения и характеристика их основных категорий;
21. Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;
22. Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;

23. Принципы организации и технического исполнения замков защиты и защиты типа «изменение функций»;
24. Классификация средства защиты с запросом информации и характеристика их основных составляющих;
25. Назначение и принцип формирования паролей, шифров, сигнатур;
26. Назначение и основные принципы построения аппаратуры защиты;
27. Классификация средств активной защиты и характеристика их основных составляющих;
28. Определение и характеристика основных внутренних средств активной защиты;
29. Определение и характеристика основных внешних средств активной защиты;
30. Классификация средств пассивной защиты и характеристика их основных составляющих;
31. Назначение и основные принципы организации идентификации программ;
32. Назначение и основные принципы построения устройств контроля;
33. Общий состав требований по обеспечению ИБ;
34. Требования к программно–аппаратным средствам;
35. Требования к подсистеме идентификации и аутентификации;
36. Требования к подсистеме управления доступом;
37. Требования к подсистеме протоколирования аудита;
38. Требования к подсистеме защиты повторного использования объектов и к защите критичной информации;

Критерии оценивания:

- оценка «отлично» - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

оценка «хорошо» - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- оценка удовлетворительно - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- оценка неудовлетворительно - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого

вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы».

Оформление лабораторных работ

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра Информационных технологий и защиты информации
(наименование кафедры)

Лабораторные работы

по дисциплине Модели разграничения доступа
(наименование дисциплины)

1. Методические рекомендации по выполнению лабораторных работ

Лабораторная работа как вид учебного занятия проводиться в специально оборудованных учебных аудиториях.

Продолжительность не менее 2-х академических часов. Необходимыми структурными элементами лабораторной работы, помимо самостоятельной

деятельности студентов, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы.

Выполнению лабораторной работы предшествует проверка знаний студентов, их теоретической готовности к выполнению задания.

По каждой лабораторной работе преподаватели должны разработать методические указания по их проведению, в соответствии с требованиями их оформления.

2. Критерии оценки:

«зачтено» выставляется студенту, если задание, предусмотренное лабораторной работой, выполнено на компьютере и студент может объяснить ее выполнение;

- «не зачтено» - выставляется студенту, если задание, предусмотренное лабораторной работой, не выполнено на компьютере или он не может объяснить ее выполнение.

4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 3 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в экзаменационном задании – 3. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры
Информационных технологий и защиты информации
Протокол №10 от «11» мая 2018 г.
Зав.кафедрой _____ Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.ОД.10 «Модели разграничения доступа»
(наименование дисциплины)

Направление подготовки

10.03.01 «Информационная безопасность»

Уровень образования
бакалавриат

Составитель _____ Скляров А.В., доцент, к.т.н.
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Основы информационной безопасности» адресованы студентам всех форм обучения.

Учебным планом по направлению подготовки «Информационная безопасность» предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные понятия и методы по дисциплине Основы информационной безопасности, даются рекомендации для самостоятельной работы и подготовке к практическим занятиям.

В ходе лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач дисциплины.

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы, помещённые в конце описания лабораторной работы.

Вопросы, не рассмотренные на лекциях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины осуществляется в ходе занятий методом устного опроса, проверки выполненных индивидуальных заданий, тестирования, проверки подготовленных конспектов по выделенным для самостоятельного изучения темам дисциплины. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных, выделить непонятные термины и найти их значение в энциклопедических словарях.

При реализации различных видов учебной работы используются разнообразные (в т.ч. интерактивные) методы обучения, в частности:

- размещение материалов курса в системе дистанционного обучения http://elearning.rsue.ru/

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронной библиотекой ВУЗа http://library.rsue.ru/. Также обучающиеся могут взять на дом необходимую литературу на абонементе вузовской библиотеки или воспользоваться читальными залами вуза.