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

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Модели разграничения доступа

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2023 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	48	48	48	48
Итого ауд.	80	80	80	80
Контактная работа	80	80	80	80
Сам. работа	28	28	28	28
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): к.ф.-м.н., доц., Шейдаков Н.Е.

Зав. кафедрой: к.э.н. доцент Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	изучить теоретические основы информационной безопасности (ИБ) и методологические нормы системного обеспечения защиты информационных процессов в компьютерных системах.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-4: способен принимать участие в проведении экспериментальных исследований объекта информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

-Физические основы программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
-принципы построения и функционирования подсистемы информационной безопасности объекта защиты (соотнесено с индикатором ПК-4.1)

Уметь:

-осуществлять научно обоснованный выбор программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
- осуществлять научно обоснованный выбор способов администрирования подсистемы информационной безопасности объекта защиты (соотнесено с индикатором ПК-4.2)

Владеть:

-методиками научно обоснованного вы-бора программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
- методиками научно обоснованного выбора способов администрирования подсистемы информационной безопасности объекта защиты (соотнесено с индикатором ПК-4.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Исходные положения теории компьютерной безопасности

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Тема 1.1. Содержание и основные понятия компьютерной безопасности Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем. Элементы теории защиты информации. Классификация угроз безопасности информации. Основные виды политик безопасности. Математические основы моделей безопасности. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
1.2	Тема 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 /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.6
1.3	Тема 1.3. Политика и модели 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 /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
1.4	Тема 1.2. Элементы теории защиты информации Математические основы моделей безопасности. Основные понятия. Элементы теории автоматов. Элементы теории графов / LibreOffice / Лаб /	7	6	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
1.5	Тема 1.2. Элементы теории защиты информации Изучение содержания и последовательности работ по защите информации. Изучить содержание и последовательность работ	7	6	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4,

	при построении комплексной системы защиты информации /LibreOffice / Лаб /				Л2.5, Л2.6
1.6	Тема 1.3. Основные составляющие моделей безопасности Математические основы моделей безопасности. Содержание и структура понятия компьютерной безопасности Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности / Ср /	7	6	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6

Раздел 2. Модели безопасности компьютерных систем

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Тема 2.1. Модели безопасности на основе дискреционной политики. Дискреционное управление доступом. Модели на основе матрицы доступа. Модели распространения прав доступа. Модель Харисона-Руззо-Ульмана (HRU-модель). Модель TAKE-GRANT. / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.2	Тема 2.2. Модели безопасности на основе мандатной политики Общая характеристика политики мандатного доступа. Модель Белла-ЛаПадулы. Основные расширения модели Белла-ЛаПадулы / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.3	Тема 2.3. Модели безопасности на основе ролевой политики Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений. Формальная спецификация и разновидности ролевых моделей. Иерархическая система ролей Взаимоисключающие роли. Количественные ограничения по ролям. Группирование ролей и полномочий. Индивидуально-групповое разграничение доступа / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.4	Тема 2.4. Модель систем военных сообщений Неформальное описание модели СВС. Формальное описание модели СВС. Безопасное состояние. Безопасность переходов. Недостатки модели. Разработка модели систем военных сообщений. / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.4, Л2.1, Л2.2, Л2.3, Л2.4, Л2.6
2.5	Тема 2.1. Модель ХРУ Модели безопасности на основе дискреционной политики. Исследование модели матрицы доступа ХРУ. Общая характеристика политики доступа. Основные расширения модели /LibreOffice / Лаб /	7	6	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.6	Тема 2.3. Исследование модели распространения прав доступа. (9 баллов) Модели безопасности на основе ролевой политики Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений /LibreOffice / Лаб /	7	6	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.7	Тема 2.3. Элементы теории защиты информации Модели безопасности на основе ролевой политики. Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений. Управление индивидуально-групповым доступом в системе на основе правила (критерия безопасности) индивидуально-группового доступа / Ср /	7	6	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6

Раздел 3. Нейтрализация скрытых каналов утечки информации на основе технологий "представлений" и "разрешенных процедур"

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
3.1	Тема 3.1. Автоматные и теоретико-вероятностные модели невлияния и невыводимости Понятие и общая характеристика скрытых каналов утечки информации. Нейтрализация скрытых каналов утечки информации на основе технологий "представлений" и "разрешенных процедур". Модели информационного	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6

	невмешательства и информационной невыводимости. Теоретико-вероятностная трактовка GM-автомата / Лек /				
3.2	Тема 3.2. Модели и технологии обеспечения целостности данных Общая характеристика моделей и технологий обеспечения целостности данных. Дискреционная модель Кларка-Вильсона. Мандатная модель Кена Биба. Технологии параллельного выполнения транзакций в клиент-серверных системах (СУБД). / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.3, Л2.4, Л2.5
3.3	Тема 3.3. Политика и модели безопасности в распределенных компьютерных системах Общая характеристика проблем безопасности в распределенных компьютерных системах. Модели распределенных систем в процессах разграничения доступа. Зональная модель разграничения доступа к информации в распределенных компьютерных системах. / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
3.4	Тема 3.1. Модель Белла-ЛаПадулы Исследование модели Белла-Ла Падула. Общая характеристика политики мандатного до-ступа Основные расширения модели Белла-ЛаПадулы /LibreOffice / Лаб /	7	6	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.3, Л2.4, Л2.5
3.5	Тема 3.2. Модель Take-Grant. Закрепление теоретического материала по модели распространения прав доступа Take-Grant, применяемой для систем защиты, использующих дискреционное разграничение доступа / LibreOffice / Лаб /	7	6	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.3, Л2.4, Л2.5
3.6	Тема 3.1. Математические основы моделей безопасности Автоматная модель невлияния Гогена-Месигера (GM-модель). Критерий безопасности в GM-модели. Основные тезисы и определения GM-модели / Ср /	7	4	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6

Раздел 4. Технологии обеспечения целостности данных

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
4.1	Тема 4.1. Методы анализа и оценки защищенности компьютерных систем Теоретико-графовые модели комплексной оценки защищенности. Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа. Теоретико-графовая модель системы индивидуально- групповых назначений доступа к иерархически организованным объектам. Пространственно-векторная модель и характеристики системы рабочих групп пользователей. / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
4.2	Тема 4.2. Стандарты информационной безопасности Первые стандарты безопасности. Оранжевая книга. Интерпретация "Оранжевой книги " для сетевых конфигураций. Рекомендации X.800. Стандарт ISO/IEC 15408. Международный стандарт ISO 17799. Российские стандарты безопасности. Гармонизированные критерии Европейских стран / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
4.3	Тема 4.3.Модель и методы качественной оценки комплексной системы информационной безопасности предприятия Задачи, принципы построения и направления работ по созданию КСИБ. Оценка рисков. Формальная модель КСИБ. Механизм функционирования КСИБ. Оценка уровня информационной безопасности. Оценка рисков. Тестирование систем информационной безопасности. / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
4.4	Тема 4.1. Модели дискреционной политики безопасности Работа с матрицей доступов. Домены безопасности. Закрепление на практике материала по дискреционным политикам безопасности, создание матрицы доступов / LibreOffice / Лаб /	7	6	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.3, Л2.4, Л2.5, Л2.6
4.5	Модели систем дискриминационного разграничения доступа Общая характеристика моделей дискреционного доступа. Пятимерное пространство Хартсона. Модели на основе матрицы доступа. Модели распространения прав доступа. Модель типизованной матрицы доступа / Ср /	7	4	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6

Раздел 5. Политика и модели безопасности в распределенных компьютерных системах					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
5.1	Тема 5.1. Методы количественной оценки систем информационной безопасности Метод экспертных оценок.Метод информационных потоков. Построение алгоритма распределения функций безопасности. Графовый метод. Метод весовых коэффициентов. / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
5.2	Тема 5.2. Комплексный подход к оценке эффективности систем информационной безопасности Качественные и количественные аспекты оценки эффективности защиты. Оценка экономической эффективности КСИБ. Обзор качественных и количественных методов / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
5.3	Тема 5.1. Мандатные политики безопасности Общая характеристика политики доступа. Исследование модели матрицы. Закрепление теоретического материала по мандатной политике безопасности / LibreOffice / Лаб /	7	6	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.6
5.4	Тема 5.1. Модели безопасности на основе тематической политики Общая характеристика тематического разграничения доступа. Тематические решетки. Модель тематико-иерархического разграничения доступа. / Ср /	7	4	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.6
Раздел 6. Методы анализа и оценки защищенности компьютерных систем					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
6.1	Тема 6.1. Теоретико-графовые модели комплексной оценки защищенности Модели комплексной оценки защищенности КС. Модель системы с полным перекрытием. Области применения теоретико-графовых моделей. Технико- экономическое обоснование систем обеспечения безопасности.Тактико-техническое обоснование систем обеспечения безопасности. / Лек /	7	2	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
6.2	Тема 6.1. Политика и модели безопасности в распределенных компьютерных системах Общая характеристика проблем безопасности в распределенных компьютерных системах. Модели распределенных систем в процессах разграничения доступа. Зональная модель разграничения доступа к информации в распределенных компьютерных системах / Ср /	7	4	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
6.3	/ Зачёт /	7	0	ПК-4	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Щербаков А.	Современная компьютерная безопасность. Теоретические основы. Практические аспекты: учебное пособие	Москва: Книжный мир, 2009	https://biblioclub.ru/index.php?page=book&id=89798 неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.2	Петренко В. И.	Теоретические основы защиты информации: учебное пособие	Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2015	https://biblioclub.ru/index.php?page=book&id=458204 неограниченный доступ для зарегистрированных пользователей
Л1.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2017	http://www.iprbookshop.ru/63594.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	https://biblioclub.ru/index.php?page=book&id=576726 неограниченный доступ для зарегистрированных пользователей
Л1.5	Бирюков А.А.	Информационная безопасность: защита и нападение	Москва: ДМК Пресс, 2017	https://ibooks.ru/reading.php?short=1&productid=364379 неограниченный доступ для зарегистрированных пользователей
5.2. Дополнительная литература				
	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Загинайлов Ю. Н.	Теория информационной безопасности и методология защиты информации: учебное пособие	Москва, Берлин: Директ-Медиа, 2015	https://biblioclub.ru/index.php?page=book&id=276557 неограниченный доступ для зарегистрированных пользователей
Л2.2		Информационная безопасность: журнал	Москва: Гротек, 2014	https://biblioclub.ru/index.php?page=book&id=364894 неограниченный доступ для зарегистрированных пользователей
Л2.3	Артемов А. В.	Информационная безопасность: курс лекций: курс лекций	Орел: Межрегиональная академия безопасности и выживания, 2014	https://biblioclub.ru/index.php?page=book&id=428605 неограниченный доступ для зарегистрированных пользователей
Л2.4		Программные продукты и системы: журнал	Тверь: Центрпрограммсистем, 2014	https://biblioclub.ru/index.php?page=book&id=459213 неограниченный доступ для зарегистрированных пользователей
Л2.5	Фомин, Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства: учебно-методическое пособие	Саратов: Вузовское образование, 2018	http://www.iprbookshop.ru/77317.html неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.6	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие к прохождению производственной практики: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	https://biblioclub.ru/index.php?page=book&id=562246 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Консультант +
ФСТЭК России/fstec.ru
ScienceDirect. https://www.sciencedirect.com/

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
LibreOffice

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-4: способен принимать участие в проведении экспериментальных исследований объекта информационной безопасности			
З: физические основы программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;- принципы построения и функционирования подсистемы информационной безопасности объекта защиты	поиск и сбор необходимой литературы, использование различных баз данных при подготовке к зачету, опросу	соответствие проблеме исследования; полнота и содержательность ответа на зачете, опросе	З – вопросы для зачёта (1-26) О – вопросы для опроса (1-14)
У: осуществлять научно обоснованный выбор программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; осуществлять научно обоснованный выбор способов администрирования подсистемы информационной безопасности объекта защиты	использование современных программно-аппаратных и технических средств при выполнении лабораторного и практико-ориентированного задания	правильный выбор программно-аппаратных и технических средств при выполнении лабораторного и практико-ориентированного задания	ПОЗЗ – практико- ориентированное задание для зачёта (1-6) ЛЗ – лабораторное задание (1-8)
В: -методиками научно обоснованного выбора программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; методиками научно обоснованного выбора способов администрирования подсистемы информационной безопасности объекта защиты	настраивает и обслуживает программно-аппаратные и технические средства при выполнении лабораторного и практико-ориентированного задания	технические средства установлены и работают корректно при выполнении лабораторного и практико-ориентированного задания	ПОЗЗ – практико- ориентированное задание для зачёта (1-6) ЛЗ – лабораторное задание (1-8)

1.2 Шкалы оценивания:

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

- 50-100 баллов («зачет»)
- 0-49 баллов («незачет).

2 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

Вопросы к зачёту

1. Основные составляющие моделей безопасности
2. Модели систем дискриминационного разграничения доступа
3. Модель матрицы доступа ХРУ
4. Модель распространения прав доступа
5. Модели систем мандатного разграничения доступа
6. Модель Белла-Ла Падула
7. Модель систем военных сообщений
8. Модели систем ролевого разграничения доступа
9. Базовая модель ролевого разграничения доступа

10. Модель администрирования ролевого разграничения доступа
11. Основные принципы архитектурной безопасности и их краткая характеристика;
12. Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;
13. Основные функции централизованного управления рисками и администрирования системы безопасности;
14. Классификация средств защиты программного обеспечения и характеристика их основных категорий;
15. Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;
16. Назначение и принцип формирования паролей, шифров, сигнатур;
17. Назначение и основные принципы построения аппаратуры защиты;
18. Классификация средств активной защиты и характеристика их основных составляющих;
19. Определение и характеристика основных внутренних средств активной защиты;
20. Определение и характеристика основных внешних средств активной защиты;
21. Классификация средств пассивной защиты и характеристика их основных составляющих;
22. Назначение и основные принципы организации идентификации программ;
23. Требования к программно–аппаратным средствам;
24. Требования к подсистеме идентификации и аутентификации;
25. Требования к подсистеме управления доступом;
26. Требования к подсистеме протоколирования аудита;

Практико-ориентированные задания к зачёту

1. Элементы теории защиты информации Математические основы моделей безопасности. Элементы теории автоматов Элементы теории графов
2. Исследование модели матрицы доступа ХРУ. Модели безопасности на основе дискреционной политики. Модель ХРУ. Основные расширения модели.
3. Исследование модели распространения прав доступа. Модели безопасности на основе ролевой политики, модель разграничения доступа на основе функционально-ролевых отношений.
4. Исследование модели Белла-Ла Падула. Общая характеристика политики мандатного доступа. Модель Белла-ЛаПадулы. Основные расширения модели Белла-ЛаПадулы.
5. Исследование модели систем военных сообщений. Общая характеристика политики мандатного доступа.
6. Исследование модели администрирования ролевого разграничения доступа Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений

Критерии оценивания:

- 50-100 баллов (зачёт)– изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленной программой курса целью обучения; правильные, уверенные действия по применению полученных навыков и умений при решении практико-ориентированного задания, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

0-49 баллов (оценка незачёт)– ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять умения и навыки при решении практико-ориентированного задания, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Вопросы для опроса

1. Элементы теории защиты информации
2. Математические основы моделей безопасности
3. Основные составляющие моделей безопасности
4. Общий состав требований по обеспечению ИБ;
5. Требования к программно–аппаратным средствам;
6. Модели систем дискриминационного разграничения доступа
7. Модель матрицы доступа ХРУ
8. Модель распространения прав доступа

9. Модели систем мандатного разграничения доступа
10. Модель Белла-Ла Падула
11. Модели систем ролевого разграничения доступа
12. Понятие ролевого разграничения доступа
13. Модель администрирования ролевого разграничения доступа
14. Основные функции защиты конечных пользователей;

Примечание: опрос проводится при проверке всех лабораторных заданий для выявления знаний при изучении соответствующих тем дисциплины в рамках текущей аттестации.

Критерии оценивания:

•2 балла выставляется обучающемуся, если изложенный материал фактически верен и логически обоснован.

•1 балл выставляется обучающемуся, если изложенный материал фактически верен, но есть незначительные ошибки.

•0 баллов, если ответ не верен

Максимальное количество баллов за семестр – 28 баллов.

Лабораторные задания

Лабораторное задание 1. Элементы теории защиты информации (9 баллов)

Математические основы моделей безопасности. Основные понятия

Элементы теории автоматов. Элементы теории графов

Лабораторное задание 2. Элементы теории защиты информации (9 баллов)

Изучение содержания и последовательности работ по защите информации.

Изучить содержание и последовательность работ при построении комплексной системы защиты информации

Лабораторное задание3. Модель ХРУ (9 баллов)

Модели безопасности на основе дискреционной политики. Исследование модели матрицы доступа ХРУ. Общая характеристика политики доступа. Основные расширения модели

Лабораторное задание 4. Исследование модели распространения прав доступа. (9 баллов)

Модели безопасности на основе ролевой политики Общая характеристика моделей разграничения доступа на основе функционально- ролевых отношений

Лабораторное задание 5. Модель Белла-ЛаПадулы (9 баллов)

Исследование модели Белла-Ла Падула. Общая характеристика политики мандатного доступа Основные расширения модели Белла-ЛаПадулы

Лабораторное задание 6. Модель Take-Grant. (9 баллов)

Закрепление теоретического материала по модели распространения прав доступа Take-Grant, применяемой для систем защиты, использующих дискреционное разграничение доступа

Лабораторное задание 7. Модели дискреционной политики безопасности (9 баллов)

Работа с матрицей доступов. Домены безопасности.

Закрепление на практике материала по дискреционным политикам безопасности, создание матрицы доступов

Лабораторное задание 8. Мандатные политики безопасности (9 баллов)

Общая характеристика политики доступа. Исследование модели матрицы. Закрепление теоретического материала по мандатной политике безопасности

Критерии оценивания:

Баллы по каждому заданию проставлены в скобках.

Распределение баллов по заданию: 9 баллов – задание выполнено верно;

8-7 баллов – при выполнении задания были допущены неточности, не влияющие на результат;

6-4 баллов – при выполнении задания были допущены ошибки;

3 - 1 балл – при выполнении задания были допущены существенные ошибки;

0 баллов – задание не выполнено.

Максимальное количество баллов за семестр – 72 балла.

3. 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. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачёта.

Зачёт проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в зачетном задании – 2. Проверка ответов и объявление результатов производится в день зачета. 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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные понятия и методы компьютерной вирусологии, даются рекомендации для самостоятельной работы и подготовке к лабораторным.

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 опроса, посредством выполнения лабораторных заданий. 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 библиотечное литературе или на электронных ресурсах.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.