МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
Заведующий кафедрой
технологий обработки и защиты информации

А.А. Сирота
24.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.53.03 Методы и стандарты оценки защищенности компьютерных систем

1.Шифр и наименование направления подготовки/специальности:
10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализации:
анализ безопасности компьютерных систем

3. Квалификация (степень) выпускника: специалист

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации

6. Составители программы:
Храмов Владимир Юрьевич, д.т.н., доцент

7. **Рекомендована:**
Научно-методическим советом ФКН, протокол № 5 от 10.03.21

8. Учебный год: 2023/2024 **Семестр(ы)**: 6

9. Цели и задачи учебной дисциплины:

Изучение теоретических основ и принципов построения защищенных систем обработки информации, стандартов информационной безопасности, критериев и классов защищенности средств вычислительной техники и автоматизированных систем, формальных моделей безопасности, методов и средств проектирования технологически безопасного программного обеспечения, порядка проведения сертификации защищенных систем обработки информации, вопросов использования интеллектуальных систем для обоснования требований и оценки защищенности систем обработки информации.

Основные задачи дисциплины:

- обучение студентов базовым понятиям стандартов информационной безопасности и руководящих документов Гостехкомиссии России (ФСТЭК России) в области защиты от НСД автоматизированных систем и средств вычислительной техники;
- обучение студентов формальным моделям безопасности для дискреционной, мандатной и ролевой политик безопасности и их расширений;
- обучение студентов базовым методам и алгоритмам проектирования технологически безопасного программного обеспечения;
- овладение практическими навыками проектирования технологически безопасного программного обеспечения и интеллектуальных систем обоснования требований и оценки защищенности систем обработки информации;
- овладение практическими навыками проведения сертификации защищенных систем обработки информации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к профессиональному циклу дисциплин и блоку дисциплин базовой профильной части. Для успешного освоения дисциплины необходимы входные знания в области устройства ЭВМ и операционных систем, принципах их работы, сетевых технологий, теории вероятностей, теории нечеткой логики, теории систем и оптимального управления, объектно-ориентированных и структурных методов проектирования программного обеспечения.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикаторы	Планируемые результаты обучения
ОПК-1.1	Способен проводить анализ защищенности и находить уязвимости компьютерной системы	ОПК-1.1.1	Знает принципы построения защищенных компьютерных систем и сетей	**Знать**: принципы построения защищенных компьютерных систем и сетей, этапы создания защищенных компьютерных систем, стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России), модели безопасности компьютерных систем, методы оценки защищенности компьютерных систем, методы проектирования защищенных компьютерных систем. **Уметь**: определять классы защищенности автоматизирванных систем и средств вычислительной техники; обосновывать требования к защищенным системам обработки информации и проводить оценку эффективности их функционирования. **Владеть**: практическими навыками применения стандартов информационной безопасности при создании защищенных систем обработки информации; навыками использования инструментальных для

				обоснования требований и оценки защищенности систем обработки информации.
		ОПК-1.1.2	Знает требования основных стандартов по оценке защищенности компьютерных систем и сетей	**Знать**: требования стандартов информационной безопасности и руководящих документы ФСТЭК России (Гостехкомиссии России по оценке защищенности компьютерных систем и сетей. **Уметь**: составлять задание по безопасности и профиль защиты при создании защищенных систем обработки информации; обосновывать требования к защищенным системам обработки информации и проводить оценку эффективности их функционирования. **Владеть**: практическими навыками применения стандартов информационной безопасности при определении уровня информационной безопасности и соответствие профилю защиты; навыками использования инструментальных интеллектуальных систем для обоснования требований и оценки защищенности систем обработки информации.
		ОПК-1.1.3	Умеет определять уровень защищенности и доверия программно-аппаратных средств защиты информации	**Знать:** требования стандартов информационной безопасности (Единые критерии безопасности информационных технологий). **Уметь**; определять уровень защищенности и доверия программно-аппаратных средств защиты информации. **Владеть**: практическими навыками использования инструментальных интеллектуальных систем для определения уровня защищенности и доверия программно-аппаратных средств защиты информации.
		ОПК-1.1.4	Умеет классифицировать информационные системы по требованиям защиты информации	**Знать:** стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России). **Уметь**; проводить классификацию информационные системы по требованиям защиты информации **Владеть**: практическими навыками классификации автоматизированных систем, средств вычислительной техники, межсетевых экранов, средств антивирусной защиты, систем обнаружения вторжений по требованиям защиты информации.
		ОПК-1.1.5	Умеет определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе	**Знать:** источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей информационных систем, формальные модели безопасности компьютерных систем, методы оценки рисков информационных систем **Уметь**; проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению **Владеть**: практическими навыками использования инструментальных средств для моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению.

		ОПК-1.1.6	Умеет выполнять анализ компьютерной системы с целью определения уровня защищенности и доверия	**знать:** стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России), формальные модели безопасности, методы обоснования требований и оценки защищенности систем обработки информации. **уметь:** определять классы защищенности автоматизированных систем и средств вычислительной техники; проводить анализ задания по безопасности и профиля защиты при анализе защищенных систем обработки информации. **владеть:**. Владеть практическими навыками применения стандартов информационной безопасности при анализе защищенных систем обработки информации; навыками использования инструментальных интеллектуальных систем для анализа требований к защищенности компьютерных систем и оценки эффективности их функционирования.
		ОПК-1.1.7	Умеет проводить теоретические исследования уровней защищенности и доверия компьютерных систем и сетей	**знать:** этапы создания защищенных компьютерных систем и сетей; формальные модели безопасности компьютерных систем; методы и средства проектирования технологически безопасного программного обеспечения; методы обоснования требований и оценки защищенности систем обработки информации. **уметь**: проводить анализ формальных моделей безопасности; оценку требований к защищенным компьютерным системам и оценку эффективности их функционирования. **владеть**: практическими навыками использования инструментальных интеллектуальных систем для оценки требований к защищенности компьютерных систем и эффективности их функционирования; практическими навыками использования CASE-средств при анализе проектных решений по обеспечению защищенности компьютерных систем.

12. Объем дисциплины в зачетных единицах/час — 4/144.
Форма промежуточной аттестации: *зачет с оценкой.*

13. Виды учебной работы:

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра 6	№ семестра	Итого
Аудиторные занятия	72	72		72
в том числе: лекции	36	36		36
практические	-	-		-
лабораторные	36	36		36
Самостоятельная работа	72	72		72
Форма промежуточной аттестации *(зачет – __ час. / экзамен – __час.)*	-	-		-
Итого:	144	144		144

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
		1. Лекции	
1.1	Стандарты информационной безопасности	1. Понятие защищенной системы обработки информации ее свойства. Методы создания безопасных систем обработки информации. 2. Критерии безопасности компьютерных систем министерства обороны США. 3. Руководящие документы Гостехкомиссии России. 4. Европейские критерии безопасности информационных технологий. 5. Федеральные критерии безопасности информационных технологий США. 6. Канадские критерии безопасности компьютерных систем. 7. Единые критерии безопасности информационных технологий. 7. Методы оценки рисков информационной безопасности. 8. Уязвимости информационных систем, их классификация и правила описания.	ЭУМК «Методы оценки безопасности КС. Проектирование защищенных ИС. Методы и стандарты оценки защищенности КС. Модели безопасности КС», 2019.
1.2	Формальные модели безопасности	9. Дискреционная и мандатная модели безопасности. 10 Модель ролевой политики безопасности.	ЭУМК
1.3	Оценка рисков информационной безопасности	11. Оценка рисков информационной безопасности систем обработки информации с использованием нечетких продукционных когнитивных карт	---
1.4	Методы и средства проектирования технологически безопасного программного обеспечения	12. Методы и средства структурного и объектно-ориентированного подходов к проектированию технологически безопасного программного обеспечения	ЭУМК
1.5	Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	13. Принципы построения, состав и структура экспертной системы с нечеткой логикой в интересах обоснования требований и оценки защищенности систем обработки информации	ЭУМК
1.6	Сертификация защищенных систем обработки информации	14. Понятие сертификации. Порядок аккредитации испытательных лабораторий и органов по сертификации. Порядок проведения сертификации	ЭУМК
		2. Практические занятия	
	нет		
		3. Лабораторные работы	
3.1	Методы и средства проектирования технологически безопасного программного обеспечения	1. Создание функциональной структурной модели защищенной системы обработки информации с использованием инструментального средства Microsoft Office Visio. 2. Создание информационной структурной модели защищенной системы обработки информации с использованием инструментального средства Microsoft Office Visio. 3. Создание функциональной объектно-ориентированной модели защищенной системы обработки информации с использованием инструментального средства Microsoft Office Visio. 4. Создание информационной объектно-ориентированной модели защищенной системы обработки информации с использованием инструментального средства Microsoft Office Visio.	---

		5. Создание событийной объектно-ориентированной модели защищенной системы обработки информации с использованием инструментального средства Microsoft Office Visio.	
3.2	Оценка рисков информационной безопасности	6. Моделирование угроз и уязвимостей систем обработки информации с использованием нечетких продукционных когнитивных карт 7. Оценка риска информационной безопасности с использованием нечетких продукционных когнитивных карт 8. Оценка риска информационной безопасности с использованием средства MATLAB.	----
3.3	Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	9. Оболочка экспертной системы с нечеткой логикой. Блок настройки на предметную область. 10. Оболочка экспертной системы с нечеткой логикой. Блок принятия решений. 11. Оценка классов защищенности автоматизированных систем от несанкционированного доступа с использованием экспертной системы с нечеткой логикой. 12. Оценка классов защищенности средств вычислительной техники с использованием оболочки экспертной системы с нечеткой логикой. 13. Обоснование требований к системам защиты информации на основе оценки параметров защищаемой информации с использованием оболочки экспертной системы с нечеткой логикой. 14. Обоснование требований к системам защиты информации на основе оценки факторов защищаемой информации с использованием оболочки экспертной системы с нечеткой логикой.	----

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Сам. работа	Всего
1	Стандарты информационной безопасности	14	-	26	40
2	Формальные модели безопасности	6		8	14
3	Оценка рисков информационной безопасности	4	8	10	22
4	Методы и средства проектирования технологически безопасного программного обеспечения	4	8	10	22
5	Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	6	20	16	42
6	Сертификация защищенных систем обработки информации	2	-	2	4
	Итого:	36	36	72	144

14. Методические указания для обучающихся по освоению дисциплины

1) При изучении дисциплины рекомендуется использовать следующие средства**:**

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и

практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций онлайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

5) При использовании дистанционных образовательных технологий и электронного обучения обучающиеся должны выполнять все указания преподавателей, вовремя подключаться к онлайн -занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2013. – 416 с.
2	Будников С.А. Информационная безопасность автоматизированных систем / С.А. Будников, Н.В. Паршин. – Воронеж: ГУП ВО «Воронежская областная типография - издательство им. Е.А. Болховитинова», 2011. – 354 с.

б) дополнительная литература:

№ п/п	Источник
3	Будников С.А. Безопасность операционных систем: учебник / С.А. Будников, В.П. Жуматий, А.В. Шабанов. – Воронеж: ВАИУ, 2009. – 360 с.
4	Климов С.М. Методы и модели противодействия компьютерным атакам / С.М. Климов. – Люберцы: КАТАЛИТ, 2008. – 316 с.
5	Хаулет Т. Защитные средства с открытыми исходными кодами / Т. Хаулет. – М.: БИНОМ, 2007. – 608 с.
6	Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А.Ю. Щербаков. – М.: Книжный мир, 2009. – 352 с.
7	Храмов В.Ю. Практикум по разработке и стандартизации программных средств и информационных технологий / В.Ю. Храмов, В.А. Скляров. – Воронеж, ВЭПИ, 2012. – 43 с.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)

№ п/п	Источник
8	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
9	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
10	«Университетская библиотека online» - Контракт № 3010-07/33-19 от 11.11.2019. «Консультант студента» - Контракт № 3010-07/34-19 от 11.11.2019. ЭБС «Лань» - Договор 3010-04/05-20 от 26.02.2020. «РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2018. ЭБС «Юрайт» - Договор № 43//8 от 10.02.2020

16. Перечень учебно-методического обеспечения для самостоятельной работы

(

№ п/п	Источник
1	Будников С.А. Информационная безопасность автоматизированных систем / С.А. Будников, Н.В. Паршин. – Воронеж: ГУП ВО «Воронежская областная типография - издательство им. Е.А. Болховитинова», 2011. – 354 с.
2	Храмов В.Ю. Практикум по разработке и стандартизации программных средств и информационных технологий / В.Ю. Храмов, В.А. Скляров. – Воронеж, ВЭПИ, 2012. – 43 с.
3	Храмов В.Ю. Система поддержки принятия решений с нечеткой логикой / Свидетельство о государственной регистрации программы для ЭВМ № 2015613774, выданное Федеральной службой по интеллектуальной собственности, патентам и товарным знакам 25.03. 2015 г

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение)

Для реализации учебного процесса используются:

1. ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.

2. ПО MATLAB Classroom ver. 7.0, 10 конкурентных бессрочных лицензий на каждый,компоненты: Matlab, Simulink, Stateflow, 1 тулбокс, N 21127/VRN3 от 30.09.2011 (за счет проекта ЕКТЕМРUS/ERAMIS).

3. ПО Матлаб в рамках подписки "Университетская лицензия на программный комплекс для ЭВМ - MathWorks, Headcount – 25 ": лицензия до 31.01.2022сублицензионный контракт 3010-07/01-19 от 09.01.19.

4. Система поддержки принятия решений с нечеткой логикой / Свидетельство о государственной регистрации программы для ЭВМ № 2015613774, выданное Федеральной службой по интеллектуальной собственности, патентам и товарным знакам 25.03. 2015 г.

5. При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 479), ПК-Intel-i3, рабочее место преподавателя: проектор, видеокоммутатор, микрофон, аудиосистема, специализированная мебель: доски меловые 2 шт., столы 60 шт., лавки 30 шт., стулья 64 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.

2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 382-385), ПК-Intel-i3 16 шт., специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства
1	Разделы 1-6 Стандарты информационной безопасности. Формальные модели безопасности.Оценка рисков информационной безопасности. Методы и средства проектирования технологически безопасного программного обеспечения. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации. Сертификация защищенных систем обработки информации	ОПК-1.1	ОПК-1.1.1	Контрольная работа (тест) по соответствующим разделам и темам. Лабораторные работы 1-14.
2	Разделы 1-6 Стандарты информационной безопасности. Формальные модели безопасности.Оценка рисков информационной безопасности. Методы и средства проектирования технологически безопасного программного обеспечения. Интеллектуальные системы обоснования требований и оценки защищенности си-	ОПК-1.1	ОПК-1.1.2	Контрольная работа (тест) по соответствующим разделам и темам. Лабораторные работы 9-14.

	стем обработки информации. Сертификация защищенных систем обработки информации			
3	Разделы 1-6 Стандарты информационной безопасности. Формальные модели безопасности.Оценка рисков информационной безопасности. Методы и средства проектирования технологически безопасного программного обеспечения. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации. Сертификация защищенных систем обработки информации	ОПК-1.1	ОПК-1.1.3	Контрольная работа (тест) по соответствующим разделам и темам. Лабораторные работы 9-14.
4	Разделы 1-6 Стандарты информационной безопасности. Формальные модели безопасности.Оценка рисков информационной безопасности. Методы и средства проектирования технологически безопасного программного обеспечения. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации. Сертификация защищенных систем обработки информации	ОПК-1.1	ОПК-1.1.4	Контрольная работа (тест) по соответствующим разделам и темам. Лабораторные работы 9-14.
5	Разделы 1-6 Стандарты информационной безопасности. Формальные модели безопасности.Оценка рисков информационной безопасности. Методы и средства проектирования технологически безопасного программного обеспечения. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации. Сертификация защищенных систем обработки информации	ОПК-1.1	ОПК-1.1.5	Контрольная работа (тест) по соответствующим разделам и темам. Лабораторные работы 6-8.
6	Разделы 1-6 Стандарты информационной безопасности. Формальные модели безопасности.Оценка рисков информационной безопасности. Методы и средства проектирования технологически безопасного программного обеспечения. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации. Сертификация защищенных систем обработки информации	ОПК-1.1	ОПК-1.16	Контрольная работа (тест) по соответствующим разделам и темам. Лабораторные работы 1-14.
7	Разделы 1-6 Стандарты информационной безопасности. Формальные модели безопасности.Оценка рисков информационной безопасности. Методы и средства проектирования технологически безопасного программного обеспечения. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации. Сертификация защищенных систем обработки информации	ОПК-1.1	ОПК-1.1.7	Контрольная работа (тест) по соответствующим разделам и темам. Лабораторные работы 1-14.

Промежуточная аттестация
Форма контроля – Зачет с оценкой
Оценочные средства для промежуточной аттестации
Перечень вопросов, практическое задание

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государ-

ственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок. Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

устный опрос на практических занятиях;

контрольная работа (тест) по теоретической части курса;

лабораторная работа.

Примерный перечень оценочных средств

№ пп	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	Устный опрос	Вопросы по темам / разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа (тест) по разделам дисциплины	Теоретические вопросы по темам / разделам дисциплины	Шкала оценивания соответствует приведенной ниже
3	Лабораторная работа	Содержит 14 лабораторных заданий	При успешном выполнении работ в течение семестра фиксируется возможность оценивания только теоретической части дисциплины в ходе промежуточной аттестации (зачета с оценкой), в противном случае проверка задания по лабораторным работам выносится на зачет.

Пример задания для выполнения лабораторной работы
Лабораторная работа №9

«Оболочка экспертной системы с нечеткой логикой. Блок настройки на предметную область»

Цель работы: привитие практических навыков построения функций принадлежности параметров защищаемой информации с использованием блока настройки на предметную область оболочки экспертной системы с нечеткой логикой.

Форма контроля: отчёт в письменном виде.

Количество отведённых аудиторных часов: 2

Задание:

Получить у преподавателя вариант задания и построить функции принадлежности для заданных параметров защищаемой информации с использованием прямых и косвенных методов экспертного опроса, реализуемых блоком настройки на предметную область оболочки экспертной системы с нечеткой логикой. Составить отчёт о проделанной работе, в котором отразить следующие пункты:

1. ФИО исполнителя и номер группы.
2. Название и цель практической работы.
3. Номер своего варианта.
4. Функции принадлежности, построенные с использованием прямых методов экспертного опроса.
5. Функции принадлежности, построенные с использованием косвенных методов экспертного опроса.

Варианты заданий. Построить функции принадлежности с использованием прямых и косвенных методов экспертного опроса, реализуемых блоком настройки на предметную область оболочки экспертной системы с нечеткой логикой, для пара-

метра защищаемой информации «время восстановления», описываемого термами «малое», «среднее», «большое» на базовой шкале от 0 до 60 минут.

Пример заданий теста по разделам дисциплины

№	Вопрос	Ответы
1	Сколько основных шагов в процедуре построения безопасных систем обработки информации ?	а) 6 б) 7 в) 4 г) 3
2	Сколько уровней адекватности определяют «Европейские критерии» ?	а) 6 б) 5 в) 7 г) 3
3	Какой показатель защищенности СВТ используется для оценки только одного класса защищенности СВТ от НСД ?	а) тестирование; б) гарантии проектирования; в) гарантии архитектуры; г) целостность.
4	Сколько классов защищенности СВТ от НСД к информации устанавливают руководящие документы ФСТЭК России ?	а) 5; б) 10; в) 12; г) 7.
5	Удовлетворяет ли функция перехода Z-системы ограничениям основной теоремы безопасности Белла-ЛаПадулы ?	а) да б) нет

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае не выполнения в течение семестра), проверку выполнения установленного перечня лабораторных заданий, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Для оценки теоретических знаний используется перечень контрольно-измерительных материалов. Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает два задания - вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.

При оценивании используется количественная шкала. Критерии оценивания представлены в приведенной ниже таблице Для оценивания результатов обучения на зачете с оценкой используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование и представление основных теоретических и практических результатов (теорем, алгоритмов, методик) с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;

3) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторно-практических заданий;

4) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

5) владение навыками программирования и экспериментирования с компьютерными моделями алгоритмов обработки информации в среде Microsoft Office Visio, Matlab и оболочки экспертной системы с нечеткой логикой в рамках выполняемых лабораторных заданий.

Критерии оценивания компетенций и шкала оценок на зачете с оценкой

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок

Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2021

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.О.52 Методы оценки безопасности компьютерных систем

Форма обучения Очное

Вид контроля Зачет с оценкой

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Критерии безопасности компьютерных систем министерства обороны США.
2. Методы и средства объектно-ориентированного подхода к проектированию технологически безопасного программного обеспечения.

…

Преподаватель _____ В.Ю. Храмов

Примерный перечень вопросов к зачету с оценкой

№	Содержание
1	Понятие защищенной системы обработки информации ее свойства
2	Методы создания безопасных систем обработки информации
3	Критерии безопасности компьютерных систем министерства обороны США
4	Руководящие документы ФСТЭК России (Гостехкомиссии России)
5	Европейские критерии безопасности информационных технологий
6	Федеральные критерии безопасности информационных технологий США
7	Канадские критерии безопасности компьютерных систем
8	Единые критерии безопасности информационных технологий

9	Методы оценки рисков информационной безопасности
10	Методы оценки защищенности систем обработки информации на основе параметров защищаемой информации
11	Методы оценки защищенности систем обработки информации на основе факторов защищаемой информации
12	Оценка рисков информационной безопасности на основе продукционных когнитивных карт
13	Оценка защищенности систем обработки информации с использованием нечетких экспертных систем
14	Дискреционные модели безопасности
15	Модель ролевой политики безопасности
16	Мандатные модели безопасности
17	Методы и средства структурного подхода к проектированию технологически безопасного программного обеспечения
18	Методы и средства объектно-ориентированного подхода к проектированию технологически безопасного программного обеспечения
19	Принципы построения системы поддержки принятия решений в интересах обоснования требований и оценки защищенности систем обработки информации
20	Состав, структура и алгоритмы функционирования системы поддержки принятия решений в интересах обоснования требований и оценки защищенности систем обработки информации
21	Понятие сертификации. Существующие правовые документы в области сертификации
22	Порядок аккредитации испытательных лабораторий и органов по сертификации.