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

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

«05» июля 2019 г.  А.А. Сирота

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.51.03 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 № 4 от 01.07.2019 г.

(отметки о продлении вносятся вручную)

8. Учебный год: 2021/2022 **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 выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-3	Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	**знать:** стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России), формальные модели безопасности; порядок сертификации защищенных 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; проверять правильность проведения сертификации 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; навыками проведения сертификации защищенных систем обработки информации.
ПК-7	Способность проводить анализ проектных решений по обеспечению за-	**знать:** этапы создания защищенных компьютерных систем; формальные модели безопасности компьютерных систем; методы и средства проектирования технологически без-

	щищенности компьютерных систем	опасного 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
ПСК-1.3	Способность использовать современные критерии и стандарты для анализа безопасности компьютерных систем	**знать:** стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России), порядок сертификации защищенных компьютерных систем; **уметь:** определять классы защищенности автоматизированных систем и средств вычислительной техники; составлять задание по безопасности и профиль защиты при создании защищенных компьютерных систем; **владеть:** практическими навыками применения стандартов информационной безопасности при создании защищенных компьютерных систем; навыками проведения сертификации защищенных компьютерных систем.

12. Объем дисциплины в зачетных единицах/час — 3/108.
Форма промежуточной аттестации: *зачет с оценкой.*

13. Виды учебной работы:

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра 6	№ семестра	Итого
Аудиторные занятия	68	68		68
в том числе: лекции	32	32		32
практические	-	-		-
лабораторные	32	32		32
Самостоятельная работа	44	44		44
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*	-	-		-
Итого:	108	108		108

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		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.
1.2	Методы и средства проектирования технологически безопасного программного обеспечения	8. Методы и средства структурного подхода к проектированию технологически безопасного программного обеспечения. 9. Методы и средства объектно-ориентированного подхода к проектированию технологически безопасного программного обеспечения.

1.3	Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	10. Принципы построения, состав и структура экспертной системы с нечеткой логикой в интересах обоснования требований и оценки защищенности систем обработки информации
1.4	Сертификация защищенных систем обработки информации	11. Понятие сертификации. Порядок аккредитации испытательных лабораторий и органов по сертификации. 12. Порядок проведения сертификации
2. Практические занятия		
2.1	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	Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	6. Оболочка экспертной системы с нечеткой логикой. Блок настройки на предметную область. 7. Оболочка экспертной системы с нечеткой логикой. Блок принятия решений. 8. Оценка классов защищенности автоматизированных систем от несанкционированного доступа с использованием экспертной системы с нечеткой логикой. 9. Оценка классов защищенности средств вычислительной техники с использованием оболочки экспертной системы с нечеткой логикой. 10. Исследование методов обоснования требований к системам защиты информации на основе оценки параметров защищаемой информации с использованием оболочки экспертной системы с нечеткой логикой. 11. Исследование методов обоснования 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	16	-	16	32
2	Методы и средства проектирования технологически безопасного программного обеспечения	4	10	10	24
3	Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	8	22	12	42
4	Сертификация защищенных систем обработки информации	4	-	6	10
	Итого:	32	32	44	108

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

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.

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

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

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:

№ 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	ЭБС «Издательства «Лань», Договор №3010-06/71-14 от 25.11.2014, ЭБС «Университетская библиотека online», Договор №3010-06/70-14 от 25.11.14, Национальный цифровой ресурс «РУКОНТ», Договор №ДС-208 от 01.02.2012

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

№ 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 инфор-

	мационных 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. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Для реализации учебного процесса используются:

1) ПО Microsoft в рамках подписок «Imagine»,ежегодные сублицензионные договоры № 56035/BPH3739 и № 56036/BPH3739 от 07.10.2016.

2) 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

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

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. Фонд оценочных средств:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ПК-3 Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знать стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России), формальные модели безопасности; порядок сертификации защищенных систем обработки информации	Разделы 1,,4 Стандарты информационной безопасности. Сертификация защищенных систем обработки информации	Устный опрос, Тест
	Уметь определять классы защищенности автоматизированных систем и средств вычислительной техники; проводить анализ задания по безопасности и профиля защиты при анализе защищенных систем обработки информации; проверять пра-	Разделы 1, 4 Стандарты информационной безопасности. Сертификация защищенных систем обработки информации	Устный опрос, Тест

	вильность проведения сертификации защищенных систем обработки информации		
	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; навыками проведения сертификации защищенных систем обработки информации.	Раздел 1, 3 Стандарты информационной безопасности. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	Лабораторные работы
ПК-7 Способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем	Знать этапы создания защищенных компьютерных систем; формальные модели безопасности компьютерных систем; методы и средства проектирования технологически безопасного программного обеспечения; методы обоснования требований и оценки защищенности систем обработки информации	Разделы 2, 3 Методы и средства проектирования технологически безопасного программного обеспечения. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	Контрольная работа по соответствующим разделам или тест
	Уметь проводить анализ формальных моделей безопасности; оценку требований к защищенным компьютерным системам и оценку эффективности их функционирования	Разделы 1, 3 Стандарты информационной безопасности. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	Контрольная работа по соответствующим разделам или тест
	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	Разделы 2, 3 Методы и средства проектирования технологически безопасного программного обеспечения. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	Лабораторные работы
ПСК-1.3 Способность использовать современные критерии и стандарты для анализа безопасности компьютерных систем	Знать стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России), порядок сертификации защищенных компьютерных систем	Разделы 1, 4 Стандарты информационной безопасности. Сертификация защищенных систем обработки информации	Контрольная работа по соответствующим разделам или тест
	Уметь определять классы защищенности автоматизированных систем и средств вычислительной техники; составлять задание по без-	Разделы 1 Стандарты информационной безопасности.	Контрольная работа по соответствующим разделам или тест

	опасности и профиль защиты при создании защищенных компьютерных систем		
	Владеть практическими навыками применения стандартов информационной безопасности при создании защищенных компьютерных систем; навыками проведения сертификации защищенных компьютерных систем.	Разделы 2, 3 Методы и средства проектирования технологически безопасного программного обеспечения. Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	Лабораторные работы
Промежуточная аттестация			Комплект КИМ

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

19.2. Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

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 и оболочки экспертной системы с нечеткой логикой в рамках выполняемых лабораторных заданий;

6) владение навыками проведения компьютерного эксперимента, тестирования компьютерных моделей безопасности.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на зачете с оценкой используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения на зачете с оценкой представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на зачете

Критерии оценивания компетенций	Уровень сформированности	Шкала оценок

	компетенций	
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

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

19.3.1 Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 19.2
3	Лабораторная работа	Содержит 11 лабораторных заданий, предусматривающих разработку моделей защищенных компьютерных систем и способность проводить инструментальный мониторинг защищенности компьютерных систем с использованием различных методов обучения.	При успешно выполнении работы ставится оценка зачтено и осуществляется допуск к зачету с оценкой, в противном случае ставится оценка не зачтено и обучающийся не допускается к зачету.
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 вопроса для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 19.2

19.3.2. Примерный перечень вопросов к зачету

№	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	Единые критерии безопасности информационных технологий.
8	Методы и средства построения структурных функциональных моделей защищенных систем обработки информации
9	Методы и средства построения структурных информационных моделей защищенных систем обработки информации
10	Методы и средства построения структурных событийных моделей защищенных систем обработки информации
11	Методы и средства построения объектно-ориентированных функциональных моделей защищенных систем обработки информации
12	Методы и средства построения объектно-ориентированных информационных моделей защищенных систем обработки информации
13	Методы и средства построения объектно-ориентированных событийных моделей защищенных систем обработки информации
14	Принципы построения экспертной системы с нечеткой логикой в интересах обоснования требований и оценки защищенности систем обработки информации
15	Состав, структура и алгоритмы функционирования системы экспертной системы с нечеткой логикой в интересах обоснования требований и оценки защищенности систем обработки информации
16	Понятие сертификации. Существующие правовые документы в области сертификации
17	Порядок аккредитации испытательных лабораторий и органов по сертификации. Порядок проведения сертификации
18	Порядок проведения сертификации

19.3.3. Пример задания для выполнения лабораторной работы

Лабораторная работа №6

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

19.3.4. 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	Сколько классов защищенности СВТ от НСД к информации устанавливают руководящие документы ФСТЭК России ?	а) 5; б) 10; в) 12; г) 7.
4	Какой показатель защищенности СВТ используется для оценки только одного класса защищенности СВТ от НСД?	а) тестирование; б) гарантии проектирования; в) гарантии архитектуры; г) целостность.
5	…	

19.3.5. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2019

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Б1.Б.52 Методы и стандарты оценки защищенности 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.

…

Контрольно-измерительный материал № 11

1. Методы и средства структурного подхода к проектированию технологически безопасного программного обеспечения.
2. Порядок аккредитации испытательных лабораторий и органов по сертификации.

…

Преподаватель _____ В.Ю. Храмов

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

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы, тесты). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 19.2.