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
03.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.56.03 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 № 7 от 03.05.23

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 — 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	72	72		72
в том числе: лекции	36	36		36
практические	-	-		-
лабораторные	36	36		36
Самостоятельная работа	36	36		36
Форма промежуточной аттестации *(зачет – __ час. / экзамен – __час.)*	-	-		-
Итого:	108	108		108

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	
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	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. 14. Обоснование требований к системам защиты информации на основе оценки факторов защищаемой информации.	----

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	-	12	26
2	Формальные модели безопасности	6		6	12
3	Оценка рисков информационной безопасности	4	8	6	18
4	Методы и средства проектирования технологически безопасного программного обеспечения	4	8	4	16
5	Интеллектуальные системы обоснования требований и оценки защищенности систем обработки информации	6	20	6	32
6	Сертификация защищенных систем обработки информации	2	-	2	4
	Итого:	36	36	36	108

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	ЭБС Лань – Лицензионный договор №3010-14/37-23 от 07.03.2023 (срок предоставления с 12.03.2023 по 11.03.2024) ЭБС «Университетская библиотека online» – Контракт №3010-06/23-22 от 30.12.2022(срок предоставления с 12.01.2023 по 11.01.2024) ЭБС «Консультант студента» – Лицензионный договор №3010-06/22-22 от 30.12.2022 (с дополнительным соглашение №1 от 09.01.2023) (срок предоставления с 12.01.2023 по 11.01.2024)

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 29.12.2018.

2. MATLAB “Total Academic Headcount – 25”. Университетская лицензия на программный комплекс для ЭВМ - MathWorks MATLAB Campus-Wide Suite по договору 3010-16/118-21 от 27.12.2021 (до 01.2025).

3. 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.

4. 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) Учебная аудитория (корп.1а, ауд. № 479): специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19’’, мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

2) Учебная аудитория (корп.1а, ауд. № 290): специализированная мебель, персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27’’ (12 шт.), мультимедийный проектор, экран.

Лабораторное оборудование искусственного интеллекта: рабочие места – персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); модули АО НПЦ «ЭЛВИС»: процессорный Салют-ЭЛ24ПМ2 (9 шт.), отладочный Салют-ЭЛ24ОМ1 (9 шт.), эмулятор MC-USB-JTAG (9 шт.).

Лабораторное оборудование электроники, электротехники и схемотехники: рабочие места – персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); стенд для практических занятий по электрическим цепям (KL-100); стенд для изучения аналоговых электрических схем (KL-200); стенд для изучения цифровых схем (KL-300).

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

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 систем обработки информации. Сертификация защищенных систем обработки информации	ОПК-1.1	ОПК-1.1.2	Контрольная работа (тест) по соответствующим разделам и темам. Лабораторные работы 9-14.
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 обоснова-	ОПК-1.1	ОПК-1.16	Контрольная работа (тест) по соответствующим разделам и темам. Лабораторные работы 1-14.

	ния требований и оценки защищенности систем обработки информации. Сертификация защищенных систем обработки информации			
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 государственного 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 параметра 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
__.__.2022

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.О.55.03 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.

…

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.

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине Б1.О.56.03 Методы и стандарты оценки защищенности компьютерных систем

Вопросы с выбором

1. Сколько классов безопасности «Европейских критериев» заимствовано из «Оранжевой книги»?

а) 2 **б)** 5 в) 3 г) 6

2. Сколько уровней адекватности определяют «Европейские критерии»?

а) 6 б) 5 **в)** 7 г) 3

3. Сколько этапов в разработке профиля защиты выделят Федеральные критерии?

а) 4 б) 3 **в)** 5

4. Какой стандарт информационной безопасности был разработан раньше ?

а) Европейские критерии;

б) Руководящие документы Гостехкомиссии России;

в) Канадские критерии.

5. Сколько групп функциональных критериев в «Канадских критериях безопасности информационных технологий» ?

а) 3 б) 2 в) 5 **г)** 4

6. Ориентирован ли продукт информационных технологий (ИТ-продукт), введенный в «Федеральных критериях…», на конкретную среду эксплуатации?

а) нет б) да

7. В каком стандарте ИБ впервые предложена концепция профиля защиты?

а) Оранжевая книга; б) Документы ГТК России;

в) Европейские критерии; г) Канадские критерии **д)** Федеральные критерии

8. В каком стандарте ИБ не устанавливается линейная шкала оценки уровня безопасности разрабатываемой системы?

а) Оранжевая книга; б) Документы ГТК России; **в)** Канадские критерии

9. В «Оранжевой книге» используются следующие категории требований:

а) политика безопасности, аудит, корректность;

б) целостность, доступность, конфиденциальность;

в) аудит, корректность, правила доступа.

10. Сколько классов безопасности «Европейских критериев» заимствовано из «Оранжевой книги»?

а) 2 **б)** 5 в) 3 г) 6

11. Сколько групп классов защищенности АС от НСД устанавливают Руководящие документы Гостехкомиссии (ФСТЭК) России?

а) 2 б) 5 **в)** 3 г) 6

12. Сколько групп классов защищенности СВТ от НСД устанавливают Руководящие документы Гостехкомиссии (ФСТЭК) России?

а) 2 **б)** 4 в) 3 г) 6

13. Сколько классов защищенности АС от НСД включает вторая группа?

а) 2 б) 4 в) 3 г) 6

14. Сколько классов защищенности СВТ от НСД включает четвертая группа?

а) 1 б) 4 в) 3 г) 2

15. Сколько классов защищенности АС от НСД к информации устанавливают Руководящие документы (РД) Гостехкомиссии (ГТК) России?

а) 7 **б)** 9 в) 6

16. Сколько классов защищенности в соответствии с РД ГТК России включает первая группа?

а) 3 б) 6 **в)** 5

17. В соответствии с РД ГТК России в классах защищенности какой группы пользователи имеют доступ ко всей информации?

а) 1 **б)** 2 **в)** 3

18. К какой группе защищенности АС от НСД к информации следует отнести АС, в которой работает один пользователь?

а) 1 б) 2 **в)** 3

19. Сколько подсистем включает СЗИ НСД в соответствии с РД ГТК России?

а) 5 б) 3 **в)** 4

20. К какой подсистеме СЗИ НСД относится функция управления потоками информации?

а) криптографическая подсистема

б) подсистема регистрации и учета

в) подсистема обеспечения целостности

г) ни к какой

21. В каком классе защищенности АС от НСД в соответствии с РД ГТК России предъявляются требования к криптографической подсистеме?

а) 2А б) 2Б в) 3А г) 1Д

22. В соответствии с РД ГТК России требования к какому классу защищенности АС от НСД сильнее?

а) 3А **б)** 2Б в) сравнивать нельзя

23. Начиная с какого класса защищенности АС от НСД в соответствии с РД ГТК России тестирование СЗИ НСД должно осуществляться не реже одного раза в квартал?

а) 2А б) 1В в) 3А **г)** 1Б

24. Требуется ли наличие администратора безопасности в классе 2Б?

а) да б) нет в) такого требования не предусмотрено

25. Какого класса СВТ должны использоваться для класса защищенности АС 1А

а) не ниже 3; **б)** не ниже 2; в) не ниже 4.

26. Сколько классов защищенности СВТ от НСД к информации содержит первая группа?

а) 5 б) 3 **в)** 1 г) 2

27. Сколько классов защищенности СВТ от НСД к информации устанавливают руководящие документы ГТК (ФСТЭК) России:

а) 5; б) 10; в) 12; **г)** 7.

28. Какой показатель защищенности СВТ используется для оценки только одного класса защищенности СВТ от НСД?

а) тестирование; б) гарантии проектирования;

в) гарантии архитектуры; г) целостность.

29. Чем характеризуется вторая группа классов защищенности СВТ от НСД к информации

а) мандатной защитой; **б)** дискреционной защитой.

30. Сколько классов защищенности СВТ от НСД характеризуется верификационной защитой?

а) 4 б) 3 **в)** 1 г) 2

31. Какого класса защищенности СВТ от НСД должны использоваться при разработке АС по требованиям класса защищенности АС от НСД 1В?

а) не ниже 4 б) не ниже 3 в) не ниже 2

32. Сколько классов защищенности межсетевых экранов (МЭ) устанавливают руководящие документы Гостехкомиссии (ФСТЭК) России?

а) 4 **б)** 5 в) 7

33. Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 1Д с внешней средой?

а) 2 б) 4 **в)** 5

34. Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 1Б с внешней средой?

а) 2 б) 4 в) 3

35. Должен ли понижаться класс защищенности АС, полученной из исходной путем добавления в нее МЭ?

а) нет б) да в) РД не определено

36. Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 3Б с внешней средой?

а) не ниже 2 б) не ниже 3 **в)** не ниже 5

37. Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 3А с внешней средой при обработке информации с грифом “секретно”?

а) не ниже 2 **б)** не ниже 3 в) не ниже 5

38. Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 2А с внешней средой при обработке информации с грифом “особой важности”?

а) не ниже 2 **б)** не ниже 1 в) не ниже 4

39. Сколько показателей защищенности используется для оценки классов защищенности МЭ?

а) 7 **б)** 12 в) 9 г) 10

40. Сколько показателей защищенности используется для оценки 5 класса защищенности МЭ?

а) 7 б) 12 **в)** 9 г) 10

41. Сколько показателей защищенности используется для оценки 4 класса защищенности МЭ?

а) 7 б) 12 в) 9 **г)** 10

42. Сколько этапов включает процесс менеджмента риска в соответствии с ГОСТ Р ИСО/МЭК 31010 – 2011?

а) 3 **б)** 5 в) 6

43. Сколько этапов включает процесс оценки риска в соответствии с ГОСТ Р ИСО/МЭК 31010 – 2011?

а) 3 б) 6 в) 2

44. На сколько групп подразделяются метолы идентификации риска в соответствии с ГОСТ Р ИСО/МЭК 31010 – 2011?

а) 2 **б)** 3 в) 5

45 На сколько групп подразделяются методы анализа риска в соответствии с ГОСТ Р ИСО/МЭК 31010 – 2011?

а) 3 б) 4 в) 5

46. Какое количество факторов, влияющих на выбор метода оценки риска, определяет ГОСТ Р ИСО/МЭК 31010 – 2011?

а) 5 б) 3 **в)** 4

47. К какой группе методов оценки риска относится метод Дельфи?

а) вспомогательные методы б) методы наблюдения

в) функциональный анализ

48. К какой группе методов оценки риска относится Марковский анализ?

а) статистические методы б) анализ сценариев

в) функциональный анализ

49. Сколько уровней контроля отсутствия недекларированных возможностей устанавливают Руководящие документы (РД) Гостехкомиссии (ГТК) России?

а) 7 **б)** 4 в) 5

50. Какой самый низкий класс межсетевых экранов в соответствии Руководящими документами ФСТЭК России?

а) 7 б) 4 **в)** 5

51. В соответствии с РД ФСТЭК России в классах защищенности АС от НСД какой группы пользователи имеют доступ ко всей информации?

а) 2 б) 4 **в)** 3

52. Сколько классов защищенности средств антивирусной защиты устанавливают РД ФСТЭК России

а) 6 б) 4 в) 3

53. Сколько классов защищенности средств обнаружения вторжений устанавливают РД ФСТЭК России

а) 3 **б)** 6 в) 4

54. Какого класса защищенности межсетевых экранов должны применяться для АС класса 3Б и 2Б?

а) не ниже 3 **б)** не ниже 5 в) не ниже 4

55. Сколько показателей качества используется при обосновании требований к системам защиты информации по параметрам защищаемой информации?

а) 3 **б)** 5 в) 4

56. Сколько показателей качества используется при обосновании требований к системам защиты информации по факторам защищаемой информации?

а) 6 б) 5 в) 4

57. Какие показатели используются при определении класса защищенности государственных информационных систем в соответствии руководящими документами ФСТЭК России?

а) конфиденциальность, целостность, доступность

б) конфиденциальность, целостность, доступность, масштаб

в) конфиденциальность, доступность, масштаб

58. Какой алгоритм вывода используется при обосновании требований к системам защиты информации на основе нечетких продукционных когнитивных карт?

а) байесовкий вывод;

б) модифицированный вывод Мамдани;

в) вывод на основе операции сравнения нечетких ситуаций.

59. Какое количество уровней конфиденциальности информации используется для обоснования требований к классам защищенности АС, СВТ, САВЗ и СОВ?

а) 4 б) 5 в) 3

60. Какой подход использован при построении экспертной системы нечеткого вывода обоснования требований и оценки защищенности систем обработки информации?

а) подход «ситуация-действие»;

б) подход «ситуация - стратегия управления – действие»

в) нейросетевая стратегия управления.

Вопросы с коротким ответом

1. Сколько классов защищенности автоматизированных систем (АС) от несанкционированного доступа (НСД) к информации устанавливают Руководящие документы (РД) Гостехкомиссии (ГТК) России (ФСТЭК России)?**) 9**

2. Сколько классов защищенности в соответствии с РД ГТК России включает первая группа? **5**

3. В соответствии с РД ГТК России в классах защищенности какой группы пользователи имеют доступ ко всей информации? **2 и 3**

4. К какой группе защищенности АС от НСД к информации следует отнести АС, в которой работает один пользователь? **3**

5. Сколько подсистем включает СЗИ от НСД в соответствии с РД ГТК России? **4**

6. Какого класса СВТ должны использоваться для класса защищенности АС 1А? **не ниже 2**.

7. Сколько классов защищенности СВТ от НСД к информации содержит первая группа? **1.**

8. Сколько классов защищенности СВТ от НСД к информации устанавливают руководящие документы ГТК России? **7.**

9. Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 1Б с внешней средой? **2**

10. Должен ли понижаться класс защищенности АС, полученной из исходной путем добавления в нее МЭ? **нет**

11. Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 3Б с внешней средой? **не ниже 5**

12. Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 3А с внешней средой при обработке информации с грифом “секретно”? **не ниже 3**

13. Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 2А с внешней средой при обработке информации с грифом “особой важности”? **не ниже 1**

14. Сколько показателей защищенности используется для оценки классов защищенности МЭ? **12**

15. Сколько показателей защищенности используется для оценки 5 класса защищенности МЭ? **9**

16. Сколько показателей защищенности используется для оценки 4 класса защищенности МЭ? **10**

17. Сколько этапов включает процесс менеджмента риска в соответствии с ГОСТ Р ИСО/МЭК 31010 – 2011? **5**

18. Сколько этапов включает процесс оценки риска в соответствии с ГОСТ Р ИСО/МЭК 31010 – 2011? **3**

19. На сколько групп подразделяются метолы идентификации риска в соответствии с ГОСТ Р ИСО/МЭК 31010 – 2011? **3**

20 На сколько групп подразделяются методы анализа риска в соответствии с ГОСТ Р ИСО/МЭК 31010 – 2011? **3**

21. Какое количество факторов, влияющих на выбор метода оценки риска, определяет ГОСТ Р ИСО/МЭК 31010 – 2011? **4**

22. К какой группе методов оценки риска относится метод Дельфи? **вспомогательные методы**

23. К какой группе методов оценки риска относится Марковский анализ? **статистические методы**

24. Сколько уровней контроля отсутствия недекларированных возможностей устанавливают Руководящие документы (РД) Гостехкомиссии (ГТК) России? **4**

25. Какой самый низкий класс межсетевых экранов в соответствии Руководящими документами ФСТЭК России? **5**

26. Сколько классов защищенности средств антивирусной защиты устанавливают РД ФСТЭК России? **6**

27. Сколько классов защищенности средств обнаружения вторжений устанавливают РД ФСТЭК России? **6**

28. Какого класса защищенности межсетевых экранов должны применяться для АС класса 3Б и 2Б? **не ниже 5**

29. Сколько показателей качества используется при обосновании требований к системам защиты информации по параметрам защищаемой информации? **5**

30. Сколько показателей качества используется при обосновании требований к системам защиты информации по факторам защищаемой информации? **6**

Вопросы с развернутым ответом

1. Определить классы защищенности автоматизированной системы (АС), средств вычислительной техники (СВТ), межсетевых экранов (МЭ), системы антивирусной защиты (САВЗ), системы обнаружения вторжений (СОВ) для АС, в которой

работает несколько пользователей с одинаковыми правами доступа и обрабатывается информация с уровнем конфиденциальности «для служебного пользования».

Ответ: АС – 2Б, СВТ – не ниже 5, МЭ – не ниже 5, САВЗ – 4, СОВ – 4.

2. Определить классы защищенности АС, СВТ, МЭ, САВЗ, СОВ для АС, в которой работает несколько пользователей с различными правами доступа и обрабатывается информация с уровнем конфиденциальности «секретно».

Ответ: АС – 1В, СВТ – не ниже 4, МЭ – не ниже 3, САВЗ – 3, СОВ – 3.

3. Определить классы защищенности АС, СВТ, МЭ, САВЗ, СОВ для АС, в которой работает один пользователь и обрабатывается информация с уровнем конфиденциальности «совершенно секретно».

Ответ: АС – 3А, СВТ – не ниже 3, МЭ – не ниже 2, САВЗ – 2, СОВ – 2.

4. Перечислите основные разделы профиля защиты.

Ответ

Профиль защиты состоит из следующих пяти разделов:

- описание;
- обоснование;
- функциональные требования к ИТ-продукту;
- требования к технологии разработки ИТ-продукта;
- требования к процессу квалификационного анализа ИТ-продукта.

5. Классы защищенности автоматизированных систем (АС) от несанкционированного доступа (НСД) к информации

Ответ

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации. Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А. Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А. Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

6. Классы защищенности средств вычислительной техники от НСД к информации

Ответ

Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс - седьмой, самый высокий - первый. Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

первая группа содержит только один седьмой класс;

вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

7. Классы защищенности межсетевых экранов от НСД к информации

Ответ

Устанавливается пять классов защищенности МЭ.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности - пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.

При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться.

Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

при обработке информации с грифом “секретно” - не ниже 3 класса;

при обработке информации с грифом “совершенно секретно” - не ниже 2 класса;

при обработке информации с грифом “особой важности” - не ниже 1 класса.

8. Классы защиты средств антивирусной защиты

Ответ

Для дифференциации требований к функциям безопасности средств антивирусной защиты установлено шесть классов защиты средств антивирусной защиты. Самый низкий класс – шестой, самый высокий – первый.

Средства антивирусной защиты, соответствующие 6 классу защиты, применяются в информационных системах персональных данных 3 и 4 классов.

Средства антивирусной защиты, соответствующие 5 классу защиты, применяются в информационных системах персональных данных 2 класса.

Средства антивирусной защиты, соответствующие 4 классу защиты, применяются в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в информационных системах персональных данных 1 класса, а также в информационных системах общего пользования II класса.

Средства антивирусной защиты, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

9. Классы защищенности средств обнаружения вторжений

Ответ

Для дифференциации требований к функциям безопасности систем обнаружения вторжений установлено шесть классов защиты систем обнаружения вторжений. Самый низкий класс - шестой, самый высокий- первый.

Системы обнаружения вторжений, соответствующие 6 классу защиты, применяются в информационных системах персональных данных 3 и 4 классов.

Системы обнаружения вторжений, соответствующие 5 классу защиты, применяются в информационных системах персональных данных 2 класса.

Системы обнаружения вторжений, соответствующие 4 классу защиты, применяются в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в информационных системах персональных данных 1 класса , а также в информационных системах общего пользования II класса.

Системы обнаружения вторжений, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

10. Группы классов защищенности АС от НСД

Рассматривается три группы.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

11. Группы классов защищенности СВТ от НСД

Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс - седьмой, самый высокий - первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

первая группа содержит только один седьмой класс;

вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

12. Определение защищенной системы обработки информации.

Под защищенной системой обработки информации понимается система, которая обладает следующими тремя свойствами:

- осуществляет автоматизацию некоторого процесса обработки конфиденциальной информации, включая все аспекты этого процесса, связанные с обеспечением безопасности обрабатываемой информации;
- успешно противостоит угрозам безопасности, действующим в определенной среде;
- соответствует требованиям и критериям стандартов информационной безопасности.

Предложенный подход к определению понятия "защищенная система" отличается от существующих в первую очередь тем, что рассматривает проблему обеспечения безопасности компьютерных систем как лежащую на стыке двух направлений: автоматизации обработки информации и общей безопасности. Это дает возможность объединить задачи автоматизации обработки конфиденциальной информации и разработки средств защиты в одну проблему создания защищенных информационных систем и в процессе ее решения применять методы и технологии, разработанные как в той, так и в другой области.

13. Основные этапы разработки защищенных систем обработки информации

Решение этой задачи осуществляется последовательным осуществлением следующих действий.

1. Определение формального механизма, адекватно выражающего заданную схему информационных потоков и правила управления ими.
2. Построение модели безопасности, отражающей заданный порядок обработки информации, и формальное доказательство ее безопасности.
3. Реализация системы обработки информации в соответствии с предложенной моделью.

4. Доказательство адекватности допустимых в автоматизированной системе потоков информации и правил управления доступом исходной схеме информационных потоков и правил управления ими.

14. Перечислите в хронологическом порядке наиболее значимые стандарты информационной безопасности.

Наиболее значимыми стандартами информационной безопасности являются (в хронологическом порядке): "Критерии безопасности компьютерных систем министерства обороны США", Руководящие документы Гостехкомиссии (ФСТЭК) России (только для нашей страны), "Европейские критерии безопасности информационных технологий", "Федеральные критерии безопасности информационных технологий США", "Канадские критерии безопасности компьютерных систем" и "Единые критерии безопасности информационных технологий".

15. Таксономия требований и критериев "Оранжевой книги"

В "Оранжевой книге" предложены три категории требований безопасности — политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних — на качество самих средств защиты.

Политика безопасности

Требование 1. Политика безопасности. Система должна поддерживать точно определенную политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основании их идентификации и набора правил управления доступом. Там, где необходимо, должна использоваться политика нормативного управления доступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации (информации, отмеченной грифом секретности — типа "секретно", "сов. секретно" и т.д.).

Требование 2. Метки. С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа. Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту.

Аудит

Требование 3. Идентификация и аутентификация. Все субъекты должен иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

Требование 4. Регистрация и учет. Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективность его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

Корректность

Требование 5. Контроль корректности функционирования средств защиты. Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление ат-

рибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

Требование 6. Непрерывность защиты. Все средства защиты (в т.ч. и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

16. Классы безопасности компьютерных систем «Оранжевой книги"

"Оранжевая книга" предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа А). Каждая группа включает один или несколько классов. Группы D и А содержат по одному классу (классы D и А соответственно), группа С — классы CI, С2, а группа В — BI, В2, В3, характеризующиеся различными наборами требований безопасности. Уровень безопасности возрастает при движении от группы D к группе А, а внутри группы — с возрастанием номера класса.

17. Для экспертной системы обоснования требований к защищенности систем обработки информации определить степень нечеткого равенства типовой и входной ситуации

S_1 = {<< 1/малый > , < 0,2/средний>, < 0/большой > / Объем информации >,
< 0,2 / малое > , < 0,8/среднее >, < 0/большое > / Время восстановления>},
S_2= {<< 0,8/малый > , < 0,4/средний>, < 0/большой > / Объем информации >,
<< 0,1 / малое > , < 0,9/среднее >, < 0/большое > / Время восстановления>}
Определить $\mu(S_1, S_2)$ при t=0,7 при наличии плохо определенных признаков.
Ответ: $\mu(S_1, S_2) = 0,8$.

18. Для экспертной системы обоснования требований к защищенности систем обработки информации определить степень нечеткого равенства типовой и входной ситуации

S_1= {<< 1/малый > , < 0,2/средний>, < 0/большой > / Объем информации >,
<< 0,2 / малое > , < 0,8/среднее >, < 0/большое > / Время восстановления>},
S_2= {<< 0,9/малый > , < 0,1/средний>, < 0/большой > / Объем информации >,
<< 0,3 / малое > , < 0,7/среднее >, < 0/большое > / Время восстановления>}
Определить $\mu(S_1, S_2)$ при t=0,7 при наличии плохо определенных признаков.
Ответ: $\mu(S_1, S_2) = 0,7$.

19. Для экспертной системы обоснования требований к защищенности систем обработки информации определить степень нечеткого равенства типовой и входной ситуации

S_1= {<< 1/малый > , < 0,2/средний>, < 0/большой > / Объем информации >,
<< 0,2 / малое > , < 0,8/среднее >, < 0/большое > / Время восстановления>},
S_2= {<< 0,4/малый > , < 1/средний>, < 0/большой > / Объем информации >,
<< 0,1 / малое > , < 0,9/среднее >, < 0/большое > / Время восстановления>}
Определить $\mu(S_1, S_2)$ при t=0,7 при наличии плохо определенных признаков.
Ответ: $\mu(S_1, S_2) = 0,2$.

20. Для экспертной системы обоснования требований к защищенности систем обработки информации определить степень нечеткого равенства типовой и входной ситуации

S_1= {<< 1/малый > , < 0,2/средний>, < 0/большой > / Объем информации >,
<< 0,2 / малое > , < 0,8/среднее >, < 0/большое > / Время восстановления>},
S_2= {<< 0,3/малый > , <1/средний>, < 0/большой > / Объем информации >,
<< 0,2 / малое > , < 0,8/среднее >, < 0/большое > / Время восстановления>}
Определить $\mu(S_1, S_2)$ при t=0,7 при наличии плохо определенных признаков.

Ответ: $\mu(S_1, S_2) = 0,2$.

21. Для экспертной системы обоснования требований к защищенности систем обработки информации определить степень нечеткого равенства типовой и входной ситуации

S_1= {<< 1/малый > , < 0,2/средний>, < 0/большой > / Объем информации >,
<< 0,2 / малое > , < 0,8/среднее >, < 0/большое > / Время восстановления>},
S_2= {<< 0,7/малый > , < 0,4/средний>, < 0/большой > / Объем информации >,
<< 0,3 / малое > , < 0,7/среднее >, < 0/большое > / Время восстановления>}
Определить $\mu(S_1, S_2)$ при t=0,7 при наличии плохо определенных признаков.

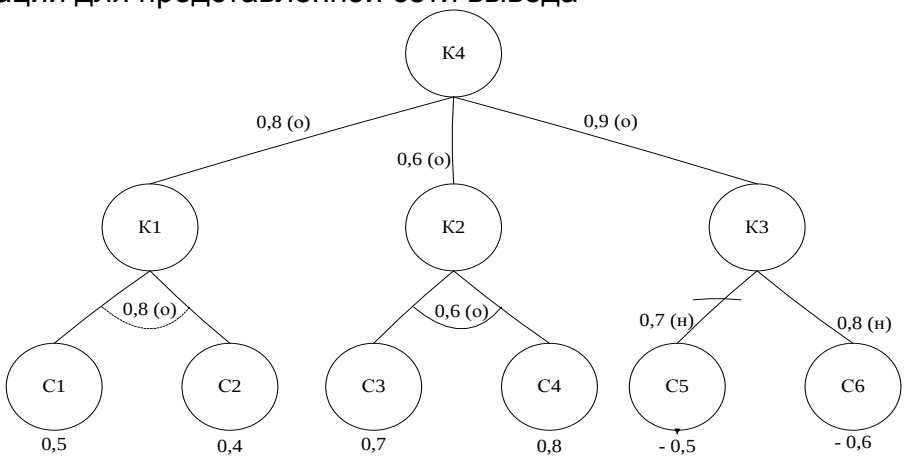
Ответ: $\mu(S_1, S_2) = 0,7$.

22. Для экспертной системы обоснования требований к защищенности систем обработки информации определить степень нечеткого равенства типовой и входной ситуации

S_1= {<< 1/малый > , < 0,2/средний>, < 0/большой > / Объем информации >,
<< 0,2 / малое > , < 0,8/среднее >, < 0/большое > / Время восстановления>},
S_2= {<< 0,7/малый > , < 0,3/средний>, < 0/большой > / Объем информации >,
<< 0,4 / малое > , < 0,6/среднее >, < 0/большое > / Время восстановления>}
Определить $\mu(S_1, S_2)$ при t=0,7 при наличии плохо определенных признаков

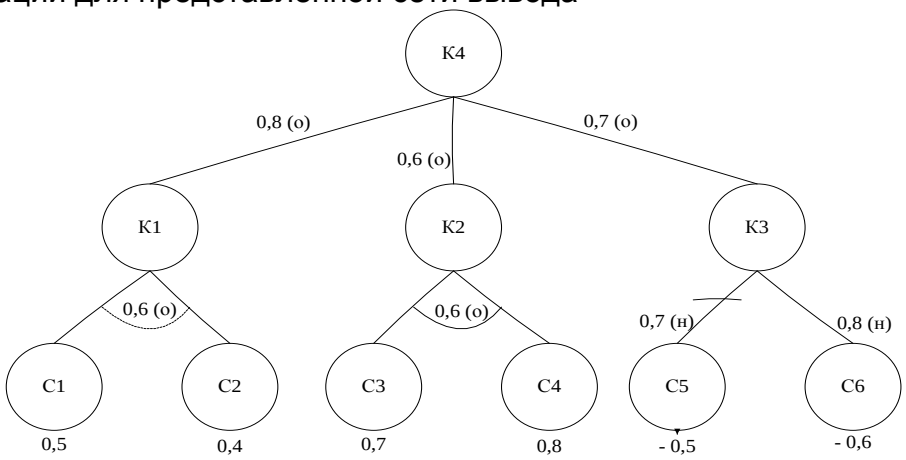
Ответ: $\mu(S_1, S_2) = 0,7$.

23. Определить вероятность гипотезы защищенности системы обработки информации для представленной сети вывода



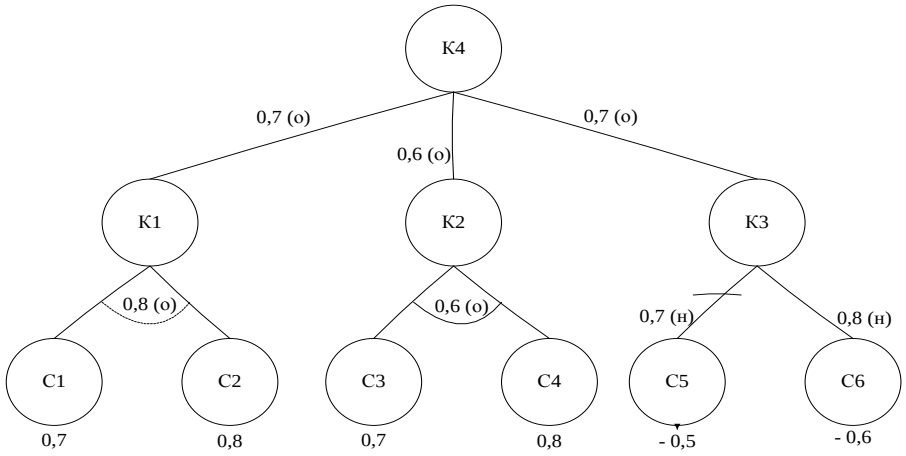
Ответ: 0,65

24. Определить вероятность гипотезы защищенности системы обработки информации для представленной сети вывода



Ответ: 0,92

25. Определить вероятность гипотезы защищенности системы обработки информации для представленной сети вывода



Ответ: 0,92

26.Приведите требования к классам защищенности автоматизированных систем в зависимости от уровня конфиденциальности обрабатываемой информации.

Уровень конфиденциальности обрабатываемой информации	Количество пользователей		
	Один пользователь	Несколько пользователей	
		Одинаковые права доступа	Различные права доступа
Особой важности	3А	2А	1А
Совершенно секретно	3А	2А	1Б
Секретно	3А	2А	1В
Для служебного пользования	3Б	2Б	1Г, 1Д

27. Классы защищенности государственных информационных систем

Ответ: Требования к классам защищенности государственных информационных систем определены Приказом ФСТЭК России № 17 от 11 февраля 2013 гола «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Класс защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

28. Как определяется уровень значимости информации для государственных информационных систем

Ответ:

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

высокой, если в результате нарушения одного из свойств безопасности инфор-

мации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

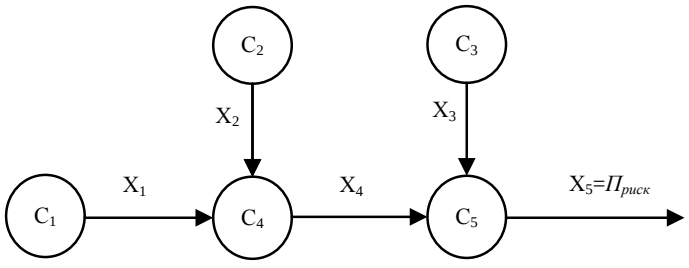
средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

29. В каких случаях уровню значимости информации для государственных информационных систем присваивается первая, вторая и третья степень?

Ответ: Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

30. Для представленной на рисунке 1 схемы НПКК с использование функций принадлежности и матриц риска, представленных на рисунках 2, 3 вычислить риск при X_1=0,85, X_2=0,9 , X_3=0,75.



C_1 – угроза; C_2 – уязвимость; C_3 – информационный ресурс; C_4 – реализация угрозы, C_5 – потенциальный ущерб, соответственно X_1 – вероятность возникновения угрозы, X_2 – вероятность наличия уязвимости; X_3 – ценность (стоимость) информационного ресурса, X_4 – вероятность успешной реализации угрозы, $X_5 = R$ – значение ожидаемого потенциального ущерба от специальных программных воздействий.

Рисунок 1 – Схема НПКК

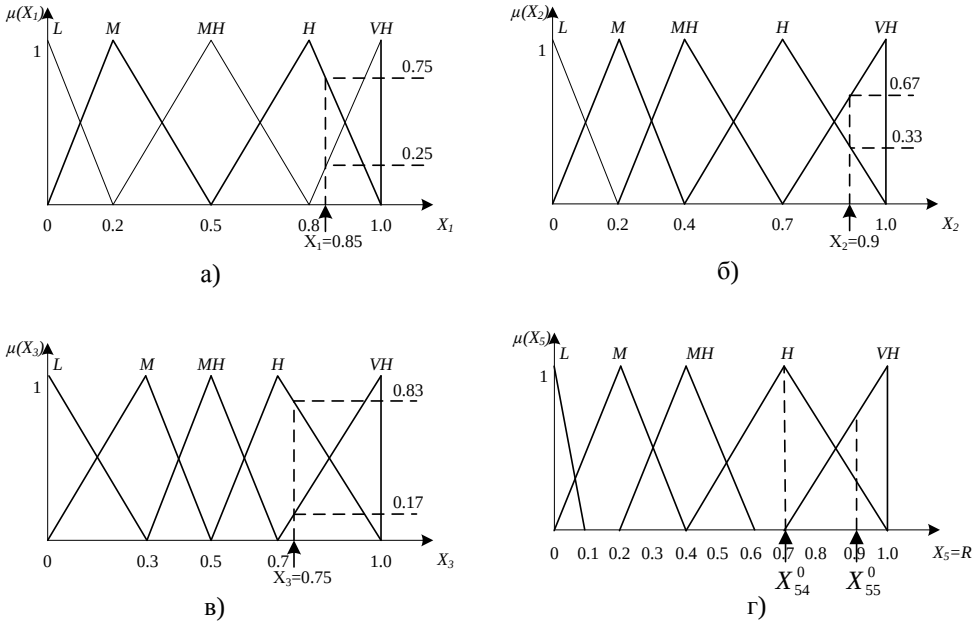


Рисунок 2 – Функции принадлежности нечетких множеств: а) угроза (C_1), б) уязвимость (C_2), в) ценность ресурса (C_3), г) потенциальный ущерб (C_5)

ct(правил)=1 *ct(правил)=1*

а) б)

Рисунок 3 – Матрицы риска: а) реализация угрозы C_4, б) потенциальный ущерб C_5

Ответ: 0,79.

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное описание заданного вопроса	Отлично (90-100 баллов)
Обучающийся приводит достаточно полное описание заданного вопроса. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Представлено описание заданного вопроса, не содержащее грубых ошибок, но не отражающее в полном объеме содержание вопроса	Удовлетворительно (50-70 баллов)
Представлено неполное описание заданного вопроса, содержащее грубые ошибки и неточности	Неудовлетворительно (менее 50 баллов)