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.38 Модели безопасности компьютерных систем

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

2. Профиль подготовки/специализации: для всех специализаций

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: 2020/2021 **Семестр(ы)**: 4

9. Цели и задачи учебной дисциплины.

Учебная дисциплина «Модели безопасности компьютерных систем» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной целью дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации; обучение общим принципам построения моделей безопасности и политик безопасности, основным методам исследования корректности систем защиты, методологии обследования и проектирования систем защиты.

Основные задачи дисциплины:

- изложение теоретических основ компьютерной безопасности;
- описание моделей безопасности информационных систем;
- описание моделей доступа в информационных системах;
- обучение методологии обследования и проектирования систем защиты;
- обучение навыкам настройки основных компонентов систем защиты и применения технологий защиты.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к профессиональному циклу дисциплин и блоку дисциплин базовой профильной части. 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	
ОПК-9	Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	**знать:** формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; **уметь:** разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; **владеть:**. практическими навыками разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах.
ПК-4	Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	**знать:** этапы создания защищенных компьютерных систем; формальные модели безопасности компьютерных систем; методы и средства обоснования требований к защищенности систем обработки информации; **уметь**: проводить анализ и разработку математических моделей безопасности компьютерных систем, обосновывать требования к защищенным компьютерным системам; **владеть**: практическими навыками разработки математических моделей безопасности компьютерных систем и обоснования требований к защищенным компьютерным системам.
ПК-10	Способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные	**знать:** стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России), методы и средства оценки эффективности реализации систем защиты информации в компьютерных системах; **уметь:** определять классы защищенности автоматизированных систем и средств вычислительной техники; применять методы и средства оценки эффективности реализации

	системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	систем защиты информации в компьютерных системах **владеть:**. практическими навыками применения стандартов информационной безопасности при создании защищенных компьютерных систем; навыками использования методов и средств оценки эффективности реализации систем защиты информации в компьютерных системах.
ПК-12	Способность проводить инструментальный мониторинг защищенности компьютерных систем	**знать:** средства инструментального мониторинга защищенности компьютерных систем; **уметь**: применять средства инструментального мониторинга защищенности компьютерных систем; **владеть**: практическими навыками применения средств инструментального мониторинга защищенности компьютерных систем.

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

13. Виды учебной работы:

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра 4	№ семестра	Итого
Аудиторные занятия	48	48		48
в том числе: лекции	16	16		16
практические	32	32		32
лабораторные	-	-		-
Самостоятельная работа	60	60		60
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*	36	36		36
Итого:	144	144		144

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. Обзор стандартов информационной безопасности.
1.2	Формальные модели безопасности	3. Базовые представления моделей безопасности. Математические основы построения моделей безопасности.
1.3	Модели компьютерных систем с дискреционным управлением	4. Дискреционная модель Харрисона-Руззо-Ульмана. Модель типизированной матрицы доступа. 5. Модель распространения прав доступа Take-Grant.
1.4	Модели компьютерных систем с мандатным управлением	6. Классическая мандатная модель Белла-ЛаПадулы. Безопасная функция перехода и уполномоченные субъекты. 7. Модели совместного доступа. Решетка мандатных моделей и их применение.
1.5	Модели компьютерных систем с ролевым управлением	8. Модель ролевой политики безопасности. 9. Ролевая политика управления доступом с иерархической организацией ролей. Примеры ролевых моделей безопасности.
1.6	Автоматные и теоретико-вероятностные модели невлияния и невыводимости	10. Модели информационного невмешательства и информационной невыводимости. 11. Нейтрализация скрытых каналов утечки информации на основе технологий"представлений" и"разрешенных процедур"
1.7	Модели безопасности на основе тематической политики	12. Общая характеристика тематического разграничения доступа. Тематические решетки.

		13. Модель тематико-иерархического разграничения доступа
1.8	Методы и средства обоснования требований и оценки защищенности компьютерных систем	14. Методы оценки параметров защищаемой информации. 15. Факторы, влияющие на требуемый уровень защиты Методы деления поля значений факторов на типовые классы. 16. Принципы построения, состав и структура экспертной системы с нечеткой логикой в интересах обоснования требований и оценки защищенности систем обработки информации
2. Практические занятия		
2.1	Стандарты информационной безопасности	1. Руководящие документы Гостехкомиссии России.
2.1	Модели компьютерных систем с дискреционным управлением	2. Дискреционная модель Харрисона-Руззо-Ульмана. 3. Модель распространения прав доступа Take-Grant
2.2	Модели компьютерных систем с мандатным управлением	4. Классическая мандатная модель Белла-ЛаПадулы
2.3	Модели компьютерных систем с ролевым управлением	5. Модель ролевого доступа при иерархически организованной системе ролей
2.4	Модели безопасности на основе тематической политики	6. Модель тематического разграничения доступа на основе иерархических рубрикаторов
2.5	Методы и средства обоснования требований и оценки защищенности компьютерных систем	7. Методы оценки параметров защищаемой информации. 8. Методы деления поля значений факторов на типовые классы. 9. Алгоритмы функционирования экспертной системы с нечеткой логикой в интересах обоснования требований и оценки защищенности систем обработки информации
3. Лабораторные работы		
3.1	нет	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Практические	Сам. работа	Всего
1	Стандарты информационной безопасности	2	4	6	12
2	Формальные модели безопасности	-	2	4	6
3	Модели компьютерных систем с дискреционным управлением	4	4	8	16
4	Модели компьютерных систем с мандатным управлением	2	4	8	14
5	Модели компьютерных систем с ролевым управлением	2	4	8	14
6	Автоматные и теоретико-вероятностные модели невлияния и невыводимости	-	4	6	10
7	Модели безопасности на основе тематической политики	2	4	8	14
8	Методы и средства обоснования требований и оценки защищенности компьютерных систем	4	6	12	22
	Итого:	16	32	60	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.
3	Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А.Ю. Щербаков. – М.: Книжный мир, 2009. – 352 с.

б) дополнительная литература:

№ п/п	Источник
4	Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие / Н.А. Гайдамакин. – Екатеринбург: УГУ им. А.М. Горького, 2008. – 212 с.
5	Будников С.А. Безопасность операционных систем: учебник / С.А. Будников, В.П. Жуматий, А.В. Шабанов. – Воронеж: ВАИУ, 2009. – 360 с.
6	Климов С.М. Методы и модели противодействия компьютерным атакам / С.М. Климов. – Люберцы: КАТАЛИТ, 2008. – 316 с.
7	Хаулет Т. Защитные средства с открытыми исходными кодами / Т. Хаулет. – М.: БИНОМ, 2007. – 608 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 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. 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)
ОПК-9 Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	Разделы 3 -,7 Модели компьютерных систем с дискреционным управлением. Модели компьютерных систем с мандатным управлением. Модели компьютерных систем с ролевым управлением. Модели безопасности информационных потоков и изолированной программной среды	Устный опрос, Тест
	Уметь разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	Разделы 2 - 7 Формальные модели безопасности. Модели компьютерных систем с дискреционным управлением. Модели компьютерных систем с мандатным управлением. Модели компьютерных систем с ролевым управлением. Модели безопасности ин-	Устный опрос, Тест

		формационных потоков и изолированной программной среды	
	Владеть практическими навыками разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	Разделы 3 - 7 Формальные модели безопасности. Модели компьютерных систем с дискреционным управлением. Модели компьютерных систем с мандатным управлением. Модели компьютерных систем с ролевым управлением. Модели безопасности информационных потоков и изолированной программной среды	Практические занятия
ПК-4 Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знать этапы создания защищенных компьютерных систем; формальные модели безопасности компьютерных систем; методы и средства обоснования требований к защищенности систем обработки информации.	Разделы 1-8 Стандарты информационной безопасности. Формальные модели безопасности. Модели компьютерных систем с дискреционным управлением. Модели компьютерных систем с мандатным управлением. Модели компьютерных систем с ролевым управлением. Модели безопасности информационных потоков и изолированной программной среды. Методы и средства обоснования требований и оценки защищенности компьютерных систем.	Контрольная работа по соответствующим разделам или тест
	Уметь проводить анализ и разработку математических моделей безопасности компьютерных систем, обосновывать требования к защищенным компьютерным системам.	Разделы 1-8 Стандарты информационной безопасности. Формальные модели безопасности. Модели компьютерных систем с дискреционным управлением. Модели компьютерных систем с мандатным управлением. Модели компьютерных систем с ролевым управлением. Модели безопасности информационных потоков и изолированной программной среды. Методы и средства обоснования требований и оценки защищенности компьютерных систем.	Контрольная работа по соответствующим разделам или тест
	Владеть практическими навыками разработки математических моделей безопасности компьютерных систем и обоснования требований к защищенным компьютерным системам.	Разделы 3-8 Модели компьютерных систем с дискреционным управлением. Модели компьютерных систем с мандатным управлением. Модели компьютерных систем с ролевым управлением. Модели безопасности информационных	Практические занятия

		потоков и изолированной программной среды. Методы и средства обоснования требований и оценки защищенности компьютерных систем.	
ПК-10 Способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России), методы и средства оценки эффективности реализации систем защиты информации в компьютерных системах.	Разделы 1, 8 Стандарты информационной безопасности. Методы и средства обоснования требований и оценки защищенности компьютерных систем.	Контрольная работа по соответствующим разделам или тест
	Уметь определять классы защищенности автоматизированных систем и средств вычислительной техники; применять методы и средства оценки эффективности реализации систем защиты информации в компьютерных системах	Разделы 1, 8 Стандарты информационной безопасности. Методы и средства обоснования требований и оценки защищенности компьютерных систем.	Контрольная работа по соответствующим разделам или тест
	Владеть практическими навыками применения стандартов информационной безопасности при создании защищенных компьютерных систем; навыками использования методов и средств оценки эффективности реализации систем защиты информации в компьютерных системах.	Разделы 1,8 Стандарты информационной безопасности. Методы и средства обоснования требований и оценки защищенности компьютерных систем.	Практические работы
ПК-12 Способность проводить инструментальный мониторинг защищенности компьютерных систем	Знать средства инструментального мониторинга защищенности компьютерных систем.	Разделы 1, 2, 8 Стандарты информационной безопасности. Формальные модели безопасности. Методы и средства обоснования требований и оценки защищенности компьютерных систем.	Контрольная работа по соответствующим разделам или тест
	Уметь применять средства инструментального мониторинга защищенности компьютерных систем.	Разделы 1, 2, 8 Стандарты информационной безопасности. Формальные модели безопасности. Методы и средства обоснования требований и оценки защищенности компьютерных систем.	Контрольная работа по соответствующим разделам или тест
	Владеть практическими навыками применения средств инструментального мониторинга защищенности компьютерных систем.	Разделы 1, 2, 8 Стандарты информационной безопасности. Формальные модели безопасности. Методы и средства обоснования требований и оценки защищенности компьютерных систем.	Практические 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 экзамене 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 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 государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на экзамене

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 прак-	Пороговый уровень	Удовлетворительно

тических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.		
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	Практическая работа	Содержит 9 практических заданий, предусматривающих разработку моделей безопасности 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 экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.
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 экзамену

№	Содержание
1	Понятие защищенной информационной системы.
2	Классификация угроз информационной безопасности.
3	Стандарты информационной безопасности.
4	Руководящие документы ФСТЭК России (Гостехкомиссии России).
5	Определение и структура политики безопасности информационной системы.
6	Формальное описание обобщённой модели системы защиты информационной системы.
7	Основные понятия защиты информации (субъекты, объекты, доступ, граф доступов, информационные потоки).
8	Модель системы безопасности Харрисона-Руззо-Ульмана (ХРУ). Основные положения модели.
9	Теорема об алгоритмической неразрешимости проблемы безопасности в произвольной системе ХРУ.
10	Модель типизированной матрицы доступов (ТМД). Основные положения модели.
11	Теорема о существовании алгоритма проверки безопасности ациклических систем монотонных ТМД.
12	Модель распространения прав доступа Take-Grant. Теоремы о передаче прав в графе доступов, состоящем из субъектов, и произвольном графе доступов.
13	Расширенная модель Take-Grant и ее применение для анализа информационных потоков в

	автоматизированной системе.
14	Модель Белла-ЛаПадулы как основа построения систем мандатного разграничения доступа. Основные положения модели.
15	Базовая теорема безопасности. Политика low-watermark в модели Белла-ЛаПадулы.
16	Применения модели Биба для реализации мандатной политики безопасности.
17	Применение модели систем военных сообщений для систем приема, передачи и обработки почтовых сообщений, реализующих мандатную политику безопасности.
18	Понятие ролевого управления доступом. Базовая модель ролевого управления доступом.
19	Понятие администрирования ролевого управления доступом. Администрирование иерархии ролей.
20	Понятие мандатного ролевого управления доступом. Требования либерального мандатного управления доступом.
21	Информационное невлияние. Информационное невлияние с учетом фактора времени.
22	Монитор безопасности объектов. Монитор безопасности субъектов.
23	Базовая теорема изолированной программной среды.

19.3.3. Пример задания для выполнения практической работы

Практическое работа № 1

«Руководящий документ Гостехкомиссии (ФСТЭК) России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»

Цель работы: привитие практических навыков определения классов защищенности автоматизированных систем от несанкционированного доступа к информации в соответствии с РД Гостехкомиссии (ФСТЭК) России

Форма контроля: отчёт в письменном виде.

Количество отведённых аудиторных часов: 2

Задание:

Получите у преподавателя вариант задания и определите класс защищенности АС от НСД к информации в соответствии с РД Гостехкомиссии (ФСТЭК) России. Составьте отчёт о проделанной работе, в котором отразите следующие пункты:

1. ФИО исполнителя и номер группы.
2. Название и цель практической работы.
3. Номер своего варианта.
4. Требования к подсистемам СЗИ от НСД к информации.
5. Класс защищенности АС от НСД к информации.

Варианты заданий. Заданы требования к подсистемам СЗИ от НСД к информации. Требуется определить класс защищенности в соответствии с РД Гостехкомиссии (ФСТЭК) России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

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	В модели изолированной программной среды, говорят, что объект о ассоциирован с субъектом s в момент времени t, когда:	а) состояние о повлияло на состояние s в момент времени t; б) состояние s повлияло на состояние о в момент времени t; в) состояние о повлияло на состояние s

		в момент времени t+1; г) состояние s повлияло на состояние o в момент времени t+1.
5	Удовлетворяет ли функция перехода Z-системы ограничениям основной теоремы безопасности Белла-ЛаПадулы?	а) да б) нет

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.38 Модели безопасности компьютерных систем

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Стандарты информационной безопасности.
2. Модель типизированной матрицы доступов. Основные положения модели.

…

Контрольно-измерительный материал № 11

1. Модель Белла-Ла Падулы как основа построения систем мандатного разграничения доступа. Основные положения модели.
2. Базовая теорема изолированной программной среды.

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.