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

УТВЕРЖДАЮ
Заведующий кафедрой
технологий обработки и защиты информации

А.А. Сирота
24.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.40 Модели безопасности компьютерных систем

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

2. Профиль подготовки/специализации:
анализ безопасности компьютерных систем

3. Квалификация выпускника: специалист

4. Форма образования: очная

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

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

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

8. Учебный год: 2022/2023 **Семестр(ы)/Трисеместры**: 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) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикаторы	Планируемые результаты обучения
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.4	знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа	**Знать**: нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа **Уметь**: применять нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа при оценке защищенности компьютерных систем **Владеть**: практическими навыками применения нормативных, руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа для проектирования, разработки и оценивания защищенности компьютерной системы.
		ОПК-6.5	знает основные угрозы безопасности информации и модели нарушителя компьютерных систем;	**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 **Уметь**; проводить классификацию угроз

				и 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-6.6	умеет разрабатывать модели угроз и модели нарушителя компьютерных систем;	**Знать:** руководящие документы ФСТЭК России (Гостехкомиссии России). **Уметь**; разрабатывать модели угроз и модели нарушителя компьютерных систем; **Владеть**: практическими навыками разработки модели угроз и модели нарушителя компьютерных систем;
		ОПК-6.8	умеет определить политику контроля доступа работников к информации ограниченного доступа	**Знать:** руководящие документы ФСТЭК России (Гостехкомиссии России). **Уметь**; определить политику контроля доступа работников к информации ограниченного доступа. **Владеть**: практическими навыками определения политики контроля доступа работников к информации ограниченного доступа.
		ОПК-6.10	умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы	**Знать:** стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России). **Уметь**; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы **Владеть**: практическими навыками применения отечественных и зарубежных стандартов в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы
ОПК-8	Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;	ОПК-8.10	умеет разрабатывать модели безопасности компьютерных систем с использованием необходимого математического аппарата и средств компьютерного моделирования	**знать:** стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России), формальные модели безопасности. **уметь:**. разрабатывать модели безопасности компьютерных систем с использованием необходимого математического аппарата и средств компьютерного моделирования **владеть:**. Владеть практическими навыками разработки моделей безопасности компьютерных систем в среде инструментальных средств
		ОПК-8.11	владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах	**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.
ОПК-11	Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;	ОПК-11.1	знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем	**знать:** основные понятия и определения, используемые при описании моделей безопасности компьютерных систем **уметь:** правильно применять основные понятия и определения при разработке формальных моделей безопасности компьютерных систем **владеть:**. практическими навыками разработки формальных моделей безопасности компьютерных систем
		ОПК-11.2	знает основные виды политик управления доступом и информационными потоками в компьютерных системах	**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
		ОПК-11.3	знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков	**знать:** основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков **уметь**: разрабатывать формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков **владеть**: практическими навыками разработки формальных модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
		ОПК-11.4	умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем	**знать:** руководящие документы ФСТЭК (Гостехкомиссии) России, определяющие модель угроз и модель нарушителя безопасности компьютерных систем **уметь**; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем

				владеть:. практическими навыками разработки модели угроз и модели нарушителя безопасности компьютерных систем
		ОПК-11.5	умеет разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	**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.

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	32	32		16
практические	16	16		32
лабораторные	-	-		-
Самостоятельная работа	60	60		60
Форма промежуточной аттестации *(Часы на контроль)*	36	36		36
Итого:	144	144		144

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Стандарты информационной безопасности	1. Понятие защищенной системы обработки информации ее свойства. Методы создания безопасных систем обработки информации 2. Обзор стандартов информационной безопасности. 3 Модели угроз и нарушителя безопасности компьютерных систем	ЭУМК «Методы оценки безопасности КС. Проектирование защищенных ИС. Методы и стандарты оценки защищенности КС. Модели безопасности КС», 2019.

1.2	Формальные модели безопасности компьютерных систем	4. Базовые представления моделей безопасности. Математические основы построения моделей безопасности. 5. Дискреционная модель Харрисона-Руззо-Ульмана. Модель типизированной матрицы доступа. 6. Модель распространения прав доступа Take-Grant. 7. Классическая мандатная модель Белла-ЛаПадулы. Безопасная функция перехода и уполномоченные субъекты. 8. Модели совместного доступа. Решетка мандатных моделей и их применение. 9. Модель ролевой политики безопасности. 10. Ролевая политика управления доступом с иерархической организацией ролей. Примеры ролевых моделей безопасности. 11. Модели информационного невмешательства и информационной невыводимости. 12. Нейтрализация скрытых каналов утечки информации на основе технологий"представлений" и"разрешенных процедур" 13. Общая характеристика тематического разграничения доступа. Тематические решетки. 14. Модель тематико-иерархического разграничения доступа 15. Модель изолированной программной среды 16. Модель безопасности информационных потоков	ЭУМК «Методы оценки безопасности КС. Проектирование защищенных ИС. Методы и стандарты оценки защищенности КС. Модели безопасности КС», 2019.
1.3	Методы и средства обоснования требований и оценки защищенности компьютерных систем	17. Принципы построения, состав и структура экспертной системы с нечеткой логикой в интересах обоснования требований и оценки защищенности систем обработки информации	ЭУМК «Методы оценки безопасности КС. Проектирование защищенных ИС. Методы и стандарты оценки защищенности КС. Модели безопасности КС», 2019.
2. Практические занятия			
2.1	Стандарты информационной безопасности	1 Руководящие документы Гостехкомиссии России. Модели угроз и нарушителя безопасности компьютерных систем	ЭУМК «Методы оценки безопасности КС. Проектирование защищенных ИС. Методы и стандарты оценки защищенности КС. Модели безопасности КС», 2019.
2.2	Формальные модели безопасности компьютерных систем	2. Дискреционная модель Харрисона-Руззо-Ульмана. 3. Модель распространения прав доступа Take-Grant 4. Классическая мандатная модель Белла-ЛаПадулы 5. Модель ролевого доступа 6. Модель изолированной программной среды 7. Модель безопасности информационных потоков 8. Модель тематического разграничения доступа на основе иерархических рубрикаторов	ЭУМК «Методы оценки безопасности КС. Проектирование защищенных ИС. Методы и стандарты оценки защищенности КС. Модели безопасности КС», 2019.
2.3	Методы и средства обоснования требований и оценки защи-	9. Экспертная система с нечеткой логикой в интересах обоснования требований и оценки защищенности компьютерных систем	ЭУМК «Методы оценки безопасности КС. Проектирование

	щенности компьютерных систем		защищенных ИС. Методы и стандарты оценки защищенности КС. Модели безопасности КС», 2019.
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	4	2	16	22
2	Формальные модели безопасности компьютерных систем	26	12	40	78
3	Методы и средства обоснования требований и оценки защищенности компьютерных систем	2	2	4	8
	Итого:	32	16	60	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	Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие / Н.А. Гайдамакин. – Екатеринбург: УГУ им. А.М. Горького, 2008. – 212 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	Будников С.А. Безопасность операционных систем: учебник / С.А. Будников, В.П. Жуматий, А.В. Шабанов. – Воронеж: ВАИУ, 2009. – 360 с.
5	Климов С.М. Методы и модели противодействия компьютерным атакам / С.М. Климов. – Люберцы: КАТАЛИТ, 2008. – 316 с.
6	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	«Университетская библиотека online» - Контракт № 3010-07/33-19 от 11.11.2019. «Консультант студента» - Контракт № 3010-07/34-19 от 11.11.2019. ЭБС «Лань» - Договор 3010-04/05-20 от 26.02.2020. «РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2018. ЭБС «Юрайт» - Договор № 43//8 от 10.02.2020

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Будников С.А. Информационная безопасность автоматизированных систем / С.А. Будников, Н.В. Паршин. – Воронеж: ГУП ВО «Воронежская областная типография - издательство им. Е.А. Болховитинова», 2011. – 354 с.
2	Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие / Н.А. Гайдамакин. – Екатеринбург: УГУ им. А.М. Горького, 2008. – 212 с.
3	Храмов В.Ю. Система поддержки принятия решений с нечеткой логикой / Свидетельство о государственной регистрации программы для ЭВМ № 2015613774, выданное Федеральной службой по интеллектуальной собственности, патентам и товарным знакам 25.03. 2015 г

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

Для реализации учебного процесса используются:

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

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

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

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

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

18. Материально-техническое обеспечение дисциплины:

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 479), ПК-Intel-i3, рабочее место преподавателя: проектор, видеокоммутатор, микрофон, аудиосисте-

ма, специализированная мебель: доски меловые 2 шт., столы 60 шт., лавки 30 шт., стулья 64 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.

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

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства
1	Разделы 1-3 Стандарты информационной безопасности. Формальные модели безопасности компьютерных систем. Методы и средства обоснования требований и оценки защищенности компьютерных систем	ОПК-6	ОПК-6.4 ОПК-6.5 ОПК-6.6 ОПК-6.7	Контрольная работа (тест) по соответствующим разделам и темам. Практическая работа 1.
2	Разделы 1-3 Стандарты информационной безопасности. Формальные модели безопасности компьютерных систем. Методы и средства обоснования требований и оценки защищенности компьютерных систем	ОПК-6	ОПК-6.10	Контрольная работа (тест) по соответствующим разделам и темам. Практические работы 1, 9.
3	Разделы 1-3 Стандарты информационной безопасности. Формальные модели безопасности компьютерных систем. Методы и средства обоснования требований и оценки защищенности компьютерных систем	ОПК-8	ОПК-8.10 ОПК-8.11	Контрольная работа (тест) по соответствующим разделам и темам. Практические работы 1-9.
4	Разделы 1-3 Стандарты информационной безопасности. Формальные модели безопасности компьютерных систем. Методы и средства обоснования требований и оценки защищенности компьютерных систем	ОПК-11	ОПК-11.1	Контрольная работа (тест) по соответствующим разделам и темам.
5	Разделы 1-3 Стандарты информационной безопасности. Формальные модели безопасности компьютерных систем. Методы и средства обоснования требований и оценки защищенности компьютерных систем	ОПК-11	ОПК-11.2 ОПК-11.3 ОПК-11.5	Контрольная работа (тест) по соответствующим разделам и темам. Практические работы 2-8.
6	Разделы 1-3 Стандарты информационной безопасности. Формальные модели безопасности компьютерных систем. Методы и средства обоснования требований и оценки защищенности компьютерных систем	ОПК-11	ОПК-11.4	Контрольная работа (тест) по соответствующим разделам и темам. Практическая работа 1.

Промежуточная аттестация
Форма контроля – Экзамен
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;

контрольная работа (тест) по теоретической части курса;

практические занятия.

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	Практическое занятие	Содержит 9 практических занятий	При успешном выполнении работ в течение семестра фиксируется возможность оценивания только теоретической части дисциплины в ходе промежуточной аттестации (экзамена), в противном случае проверка задания по практике выносится на экзамен.

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 несанкциониро-

ванного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

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 o ассоциирован с субъектом s в момент времени t, когда:	а) состояние o повлияло на состояние s в момент времени t; б) состояние s повлияло на состояние o в момент времени t; в) состояние o 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

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 Matlab и оболочки экспертной системы с нечеткой логикой.

Критерии оценивания компетенций и шкала оценок на зачете с оценкой

Критерии оценивания компетенций	Уровень сформированности	Шкала оценок

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

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2021

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Б1.О.40 Модели безопасности компьютерных систем

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

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

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 си-

	стеме 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.