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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2025

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.40 Модели безопасности компьютерных систем

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

2. Специализация:
Математические методы защиты информации

3. Квалификация (степень) выпускника: специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кибербезопасности информационных систем

6. Составители программы: Сафронов Виталий Владимирович, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована: НМС факультета ПММ, протокол № 6 от 17.03.2025

_____
отметки о продлении вносятся вручную)

8. Учебный год: 2026/2027 **Семестр(ы): 4**

9. Цели и задачи учебной дисциплины.

Целями освоения учебной дисциплины являются:

изучение принципов и методов оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности в таких системах в рамках обеспечения безопасности информационных систем и технологий в целом, изучение математических основ моделирования процессов оценки безопасности компьютерных систем, получение профессиональных компетенций в области современных технологий оценки безопасности компьютерных систем.

Задачи учебной дисциплины:

- обучение студентов базовым понятиям современных методов оценки безопасности компьютерных систем;
- обучение студентов базовым методам оценки безопасности компьютерных систем;
- овладение практическими навыками применения методов оценки безопасности компьютерных систем;
- раскрытие физической сущности построения и эксплуатации компьютерных систем с точки зрения определения актуальных угроз безопасности в таких системах с целью корректного решения задач по применению методов оценки безопасности компьютерных систем.

10.Место учебной дисциплины в структуре ОПОП:

Обязательная часть блока Б1. 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 — 3/108.
Форма промежуточной аттестации: экзамен.

13. Трудоемкость по видам 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	24	24		24
Форма промежуточной аттестации *(Часы на контроль)*	36	36		36
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. Обзор стандартов информационной безопасности. 3 Модели угроз и нарушителя безопасности компьютерных систем	ЭУМК https://edu.vsu.ru/course

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	«https://edu.vsu.ru/course
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	https://edu.vsu.ru/course
2. Практические занятия			
2.1	Стандарты информационной безопасности	1 Руководящие документы Гостехкомиссии России. Модели угроз и нарушителя безопасности компьютерных систем	https://edu.vsu.ru/course
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	https://edu.vsu.ru/course
2.3	Методы и средства обоснования требований и оценки защищенности компьютерных систем	9. Экспертная система с нечеткой логикой в интересах обоснования требований и оценки защищенности компьютерных систем	https://edu.vsu.ru/course
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	4	10
2	Формальные модели безопасности компьютерных систем	26	12	16	54
3	Методы и средства обоснования требований и оценки защищенности компьютерных систем	2	2	4	8
	Итого:	32	16	24	72

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/)

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.
2. ПО MATLAB.
3. 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:

Лекционная аудитория должна быть оборудована учебной мебелью, компьютером, мультимедийным оборудованием (проектор, экран, средства звуковоспроизведения), допускается переносное оборудование.

Для самостоятельной работы необходимы компьютерные классы, помещения, оснащенные компьютерами с доступом к сети Интернет.

Программное обеспечение (см. файл МТО)

1. ПО Microsoft.
2. ПО MATLAB.
3. 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.

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, определя- ющие процедуры оценивания

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; защиты лабораторных работ, выполнения контрольных работ.
Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования. Промежуточная аттестация по итогам освоения дисциплины проводится в форме зачета с оценкой и экзамена. Для получения положительной итоговой оценки необходимо выполнение всех лабораторных и контрольных работ

20.1.Текущий контроль успеваемости

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

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

устный опрос;

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 несанкционированного 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 и итоговая 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 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 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

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.

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.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

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;

1) закрытые задания (тестовые, средний уровень сложности):

B1

Мощность какого множества модели ХРУ больше: субъектов или объектов ?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	субъектов		*0*
B.	объектов		*100*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B10

Какая ролевая модель реализует статическое разделение обязанностей?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**

Какая ролевая модель реализует статическое разделение обязанностей?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	модель с иерархической организацией ролей		*0*
B.	модель с ограничениями на одновременное использование ролей в одном сеансе		*0*
C.	модель со взаимоисключающими ролями		*100*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B11

Какими понятиями замещается понятие «субъект» в ролевой модели?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	объект		*0*
B.	пользователь		*100*
C.	сущность		*0*
D.	роль		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B12

Что означает правило управления доступом user в ролевой модели?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**

Что означает правило управления доступом user в ролевой модели?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	для каждого сеанса определяет пользователя, который осуществляет этот сеанс работы с системой		*100*
B.	для каждого сеанса задает набор доступных в нем полномочий, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе		*0*
C.	для каждого сеанса определяет набор ролей, которые могут быть одновременно доступны пользователю в этом сеансе		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B13

Какая ролевая модель реализует динамическое разделение обязанностей?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	модель с иерархической организацией ролей		*0*
B.	модель с ограничениями на одновременное использование ролей в одном сеансе		*100*
C.	модель со взаимоисключающими ролями		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B14

К какому классу моделей безопасности относится модель Take-Grant?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**

К какому классу моделей безопасности относится модель Take-Grant?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	дискреционные модели безопасности		*100*
B.	мандатные модели безопасности		*0*
C.	ролевые модели безопасности		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B15

К какому классу моделей безопасности относится модель типизированной матрицы доступа?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	дискреционные модели безопасности		*100*
B.	мандатные модели безопасности		*0*
C.	ролевые модели безопасности		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

2) открытые задания (тестовые, средний уровень сложности):

K1

Сколько примитивных (элементарных) операций используется в классической модели XPУ?			*SA*
		Балл по умолчанию:	1
		Чувствительность к регистру:	Нет
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
	Ответы	**Отзыв**	**Оценка**
	6		*100*
	Общий отзыв к вопросу:		
	Подсказка 1:		
	Теги:		
Вам необходимо указать хотя бы один возможный ответ. Пустые ответы не будут использоваться. Символ «» можно использовать в качестве шаблона, соответствующего любым символам. Первый подходящий ответ будет использоваться для определения оценки и отзыва.*			

K2

Удовлетворяет ли функция перехода Z-системы ограничениям основной теоремы безопасности Белла-ЛаПадулы?	*SA*

		Балл по умолчанию:	1
		Чувствительность к регистру:	Нет
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
	Ответы	**Отзыв**	**Оценка**
	да		*100*
	Общий отзыв к вопросу:		
	Подсказка 1:		
	Теги:		
Вам необходимо указать хотя бы один возможный ответ. Пустые ответы не будут использоваться. Символ «» можно использовать в качестве шаблона, соответствующего любым символам. Первый подходящий ответ будет использоваться для определения оценки и отзыва.*			

К3

Чем является ячейка матрицы доступа модели ХРУ?			*SA*
		Балл по умолчанию:	1
		Чувствительность к регистру:	Нет
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
	Ответы	**Отзыв**	**Оценка**
	множеством		*100*
	Общий отзыв к вопросу:		
	Подсказка 1:		
	Теги:		
Вам необходимо указать хотя бы один возможный ответ. Пустые ответы не будут использоваться. Символ «» можно использовать в качестве шаблона, соответствующего любым символам. Первый подходящий ответ будет использоваться для определения оценки и отзыва.*			

ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

1) закрытые задания (тестовые, средний уровень сложности):

В16

К какому классу моделей безопасности относится модель Белла-ЛаПадулы?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	дискреционные модели безопасности		*0*
B.	мандатные модели безопасности		*100*
C.	ролевые модели безопасности		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

В17

К какому классу моделей безопасности относится модель безопасности переходов?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**

К какому классу моделей безопасности относится модель безопасности переходов?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	дискреционные модели безопасности		*0*
B.	мандатные модели безопасности		*100*
C.	ролевые модели безопасности		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B18

Сколько примитивных (элементарных) операций используется в классической модели XPУ?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	4		*0*
B.	6		*100*
C.	5		*0*
D.	7		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B19

К какому классу операций относится операция Create классической модели XPУ?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**

К какому классу операций относится операция Create классической модели ХРУ?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	монотонная		*100*
B.	немонотонная		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B2

Сколько основных множеств использует ролевая модель для описания системы?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	5		*0*
B.	4		*100*
C.	3		*0*
D.	7		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B20

В каком случае задача проверки безопасности системы ХРУ является разрешимой?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**

В каком случае задача проверки безопасности системы ХРУ является разрешимой?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	система команд не содержит элементарных операций «удалить» и «уничтожить»		*0*
B.	команды являются монооперационными		*100*
C.	команды системы являются одноусловными и монотонными		*100*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B21

Сколько функций уровня безопасности используется в модели безопасности переходов?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	3		*0*
B.	2		*100*
C.	1		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

2) открытые задания (тестовые, средний уровень сложности):

K4

Как изменяется матрица доступа при выполнении команды **create subject** s (создание нового субъекта s) в модели ХРУ?			*SA*
		Балл по умолчанию:	1
		Чувствительность к регистру:	Нет
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
	Ответы	**Отзыв**	**Оценка**
	Добавляется новая строка и новый столбец		*100*
	Общий отзыв к вопросу:		
	Подсказка 1:		
	Теги:		
Вам необходимо указать хотя бы один возможный ответ. Пустые ответы не будут использоваться. Символ «» можно использовать в качестве шаблона, соответствующего любым символам. Первый подходящий ответ будет использоваться для определения оценки и отзыва.*			

К5

Как изменяется матрица доступа при выполнении команды **create object** о (создание нового объекта о) в модели ХРУ?			*SA*
		Балл по умолчанию:	1
		Чувствительность к регистру:	Нет
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
	Ответы	**Отзыв**	**Оценка**
	Добавляется новый столбец		*100*
	Общий отзыв к вопросу:		
	Подсказка 1:		
	Теги:		
Вам необходимо указать хотя бы один возможный ответ. Пустые ответы не будут использоваться. Символ «» можно использовать в качестве шаблона, соответствующего любым символам. Первый подходящий ответ будет использоваться для определения оценки и отзыва.*			

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;

1) закрытые задания (тестовые, средний уровень сложности):

В3

Состояние в модели Белла-ЛаПадулы называется безопасным по чтению, если			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	уровень безопасности субъекта не ниже уровня безопасности объекта		*100*
B.	уровень безопасности объекта не ниже уровня безопасности субъекта		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

В4

Система ХРУ называется монооперационной, если			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**

Система ХРУ называется монооперационной, если			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	система команд не содержит элементарных операций «удалить» и «уничтожить»		*0*
B.	каждая команда системы содержит одну элементарную операцию		*100*
C.	команды системы являются одноусловными		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B5

Удовлетворяет ли функция перехода Z-системы ограничениям основной теоремы безопасности Белла-ЛаПадулы?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	да		*100*
B.	нет		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B6

Ячейка матрицы доступа модели ХРУ является			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**

Ячейка матрицы доступа модели ХРУ является			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	строкой		*0*
B.	множеством		*100*
C.	числом		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B7

Какое дополнительное отношение на множестве ролей вводится в ролевой модели с иерархической организацией ролей?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	отношение строгого порядка		*0*
B.	отношение эквивалентности		*0*
C.	отношение толерантности		*0*
D.	отношение нестрогого порядка		*100*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B8

Какое количество базовых представлений включают в себя модели безопасности?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**

Какое количество базовых представлений включают в себя модели безопасности?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	4		*0*
B.	6		*100*
C.	7		*0*
D.	5		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

B9

Существует ли алгоритм проверки безопасности произвольной системы ХРУ?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Да
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	33.3
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	да		*0*
B.	нет		*100*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

2) открытые задания (мини-кейсы, средний уровень сложности):

P1

Приведите основные элементарные операции модели ХРУ			*ES*
		Балл по умолчанию:	1
		Формат ответа:	HTML-редактор
		Требовать текст:	Да
		Размер поля:	15
		Разрешить вложения:	0
		Требуемое число вложений:	0
		Разрешенные типы файлов:	
		ID-номер:	
	Шаблон ответа	**Информация для оценивающих**	
	Общий отзыв к вопросу:		
	Теги:		
Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.			

P2

Приведите пример команды создания субъектом s личного файла f в модели XPУ			*ES*
		Балл по умолчанию:	1
		Формат ответа:	HTML-редактор
		Требовать текст:	Да
		Размер поля:	15
		Разрешить вложения:	0
		Требуемое число вложений:	0
		Разрешенные типы файлов:	
		ID-номер:	
	Шаблон ответа	**Информация для оценивающих**	
	Общий отзыв к вопросу:		
	Теги:		
Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.			

P3

Приведите пример команды передачи субъекту s' права read на файл f его владельцем субъектом s			*ES*
		Балл по умолчанию:	1
		Формат ответа:	HTML-редактор
		Требовать текст:	Да
		Размер поля:	15
		Разрешить вложения:	0
		Требуемое число вложений:	0
		Разрешенные типы файлов:	
		ID-номер:	
	Шаблон ответа	**Информация для оценивающих**	
	Общий отзыв к вопросу:		
	Теги:		
Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.			

P4

Приведите определение безопасного состояния, предложенного Белл и ЛаПадула			*ES*
		Балл по умолчанию:	1
		Формат ответа:	HTML-редактор
		Требовать текст:	Да
		Размер поля:	15
		Разрешить вложения:	0
		Требуемое число вложений:	0
		Разрешенные типы файлов:	
		ID-номер:	
	Шаблон ответа	**Информация для оценивающих**	
	Общий отзыв к вопросу:		
	Теги:		
Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.			

P5

Сформулируйте основную теорему безопасности Белла-ЛаПадулы			*ES*
		Балл по умолчанию:	1
		Формат ответа:	HTML-редактор
		Требовать текст:	Да
		Размер поля:	15
		Разрешить вложения:	0
		Требуемое число вложений:	0
		Разрешенные типы файлов:	
		ID-номер:	
	Шаблон ответа	**Информация для оценивающих**	
	Общий отзыв к вопросу:		
	Теги:		
Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.			

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).