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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

17.03.2025

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

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

"Безопасность компьютерных систем и сетей" (по отрасли или в сфере профессиональной деятельности)

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

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: дисциплина относится к обязательной части блока Б1.

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(ы)	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-6.1	знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации	Знать: – нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; – 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; – руководящие документы ФСТЭК России (Гостехкомиссии России); – нормативные документы ФСТЭК России (Гостехкомиссии России); – стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России). Уметь: – применять нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа при оценке защищенности компьютерных систем; – проводить классификацию угроз и уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; – разрабатывать модели угроз и модели нарушителя компьютерных
		ОПК-6.2	знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях	
		ОПК-6.3	знает систему организационных мер, направленных на защиту информации ограниченного доступа	
		ОПК-6.4.	Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа.	
		ОПК-6.5.	Знает основные угрозы безопасности информации и модели нарушителя компьютерных систем.	

		ОПК-6.6.	Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем.	систем; – определить политику контроля доступа работников к информации ограниченного доступа; – применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы. 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; – практическими навыками использования инструментальных средств для моделирования угроз безопасности в компьютерных системах с учетом мер по их предотвращению; – практическими навыками разработки модели угроз и модели нарушителя компьютерных систем; – практическими навыками определения политики контроля доступа работников к информации ограниченного доступа; – практическими навыками применения отечественных и зарубежных стандартов в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.
		ОПК-6.7	умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	
		ОПК-6.8.	Умеет определить политику контроля доступа работников к информации ограниченного доступа.	
		ОПК-6.9	умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	
		ОПК-6.10.	Умеет применять отечественные и зарубежные стандарты 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; – 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: – разрабатывать модели безопасности компьютерных систем с использованием необходимого математического аппарата и средств компьютерного моделирования; – проводить анализ формальных моделей безопасности; оценку требований к защищенным компьютерным системам и оценку эффективности их функционирования. Владеть: – практическими навыками разработки моделей безопасности компьютерных систем в среде инструментальных
		ОПК-8.11.	Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.	

				средств; – 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; – формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; – основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; – руководящие документы ФСТЭК (Гостехкомиссии) России, определяющие модель угроз и модель нарушителя безопасности компьютерных систем уметь; разрабатывать модели угроз и – модели нарушителя безопасности компьютерных систем; – формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах. Уметь: – правильно применять основные понятия и определения при разработке формальных моделей безопасности компьютерных систем; – разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; – разрабатывать формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; – разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах. Владеть: – практическими навыками разработки формальных моделей безопасности компьютерных систем; – практическими навыками разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; – практическими навыками разработки формальных модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности
		ОПК-11.2.	Знает основные виды 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.	
		ОПК-11.4.	Умеет разрабатывать 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.	

				информационных потоков; – практическими навыками разработки модели угроз и модели нарушителя безопасности компьютерных систем; – практическими навыками разработки формальных моделей политик безопасности, политик управления доступом и информационными по токами 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	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
				4		
Аудиторные занятия	48			48		
в том числе: лекции	32			32		
Практические	16			16		
Лабораторные	0			0		
Самостоятельная работа	24			24		
Контроль	36			36		
Итого:	108			108		
Форма промежуточной аттестации	Экзамен			Экзамен		

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	Б1.О.40 Модели безопасности компьютерных систем (10.05.01 БКСиС_ММЗИ)
1.2	Формальные модели без опасности компьютерных систем	1. Базовые представления моделей безопасности. Математические основы построения моделей безопасности. 2. Дискреционная модель Харрисона-РуззоУльмана. Модель типизированной матрицы доступа. 3. Модель распространения прав доступа TakeGrant. 4. Классическая мандатная модель Белла-ЛаПадулы. Безопасная функция перехода и уполномоченные субъекты. 5. Модели совместного доступа. Решетка мандатных моделей и их применение. 6. Модель ролевой политики безопасности. 7. Ролевая политика управления доступом с иерархической организацией ролей. Примеры ролевых моделей безопасности.	

		8. Модели информационного невмешательства и информационной невыводимости. 9. Нейтрализация скрытых каналов утечки информации на основе технологий "представлений" и "разрешенных процедур" 10. Общая характеристика тематического разграничения доступа. Тематические решетки. 11. Модель тематико-иерархического разграничения доступа 12. Модель изолированной программной среды 13. Модель безопасности информационных потоков.	
1.3	Методы и средства обоснования требований и оценки защищенности компьютерных систем	1. 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 Модели угроз и нарушителя безопасности компьютерных систем	Б1.О.40 Модели безопасности компьютерных систем (10.05.01 БКСиС_ММЗИ)
2.2	Формальные модели безопасности компьютерных систем	1. Дискреционная модель Харрисона-Руззо-Ульмана. 2. Модель распространения прав доступа Take-Grant. 3. Классическая мандатная модель Белла-ЛаПадулы. 4. Модель ролевого доступа. 5. Модель изолированной программной среды. 6. Модель безопасности информационных потоков. 7. Модель тематического разграничения доступа на основе иерархических рубрикаторов.	
2.3	Методы и средства обоснования требований и оценки защищенности компьютерных систем	1. Экспертная система с нечеткой логикой в интересах обоснования требований и оценки защищенности компьютерных систем.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Стандарты информационной безопасности	4	2	0	4	12	22
1.2	Формальные модели безопасности компьютерных систем	26	12	0	16	16	70
1.3	Методы и средства обоснования требований и оценки защищенности компьютерных систем	2	2	0	4	8	16
	Итого:	32	16	0	24	36	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, практические занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Практические занятия предназначены для формирования умений и навыков,закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку кэкзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

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

а) основная литература:

№ п/п	Источник
1	Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299.
2	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401.
3	Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие / Н.А. Гайдамакин. – Екатеринбург: УГУ им. А.М. Горького, 2008. – 212 с.
4	Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А.Ю. Щербаков. – М.: Книжный мир, 2009. – 352 с.
5	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. посо- бие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2013. – 416 с.

б) дополнительная литература:

№ п/п	Источник
6	Будников С.А. Безопасность операционных систем: учебник / С.А. Будников, В.П. Жума- тий, А.В. Шабанов. – Воронеж: ВАИУ, 2009. – 360 с.
7	Климов С.М. Методы и модели противодействия компьютерным атакам / С.М. Климов. – Люберцы: КАТАЛИТ, 2008. – 316 с.
8	Хаулет Т. Защитные средства с открытыми исходными кодами / Т. Хаулет. – М.: БИНОМ, 2007. – 608 с.

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
9	Электронно-библиотечная система «Университетская библиотека online (доступ осуществляется по адресу: https://biblioclub.ru/);
10	Информационно-телекоммуникационная система «Контекстум» (Национальный цифровой ресурс «РУКОНТ»);
11	Электронно-библиотечной системе «Лань» (доступ осуществляется по адресу: https://e.lanbook.com/),
12	ЭБС «BOOK» (доступ осуществляется по адресу: https://book.ru).
13	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
14	Б1.О.40 Модели безопасности компьютерных систем (10.05.01 БКСиС_ММЗИ)/Сафронов В.В. - Образовательный портал «Электронный университет ВГУ».

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются

методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по практическим работам, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий практических работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

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

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Б1.О.40 Модели безопасности компьютерных систем (10.05.01 БКСиС_ММЗИ)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15 в.14.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий *лекционного типа*, семинарского типа, организации самостоятельной работы, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации: специализированная мебель, компьютер (ноутбук), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения), допускается использование переносного оборудования.

ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office, Notepad ++ (свободное и/или бесплатное ПО), 7-zip (свободное и/или бесплатное ПО).

Учебная аудитория для проведения *практических занятий,* лабораторных работ, *организации самостоятельной работы*, проведения текущей и промежуточной аттестаций: специализированная мебель, персональные компьютеры для индивидуальной работы с возможностью подключения к сети «Интернет», мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).

ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office), специализированное ПО по тематике дисциплины (допускается демоверсия или виртуальный аналог ПО), Intellij IDEA Community Edition (свободное и/или бесплатное ПО); Jet Brains PyCharm Community Edition (свободное и/или бесплатное ПО); Anaconda (свободное и/или бесплатное ПО); Maxima (свободное и/или бесплатное ПО); Scilab (свободное и/или бесплатное ПО); NetBeans IDE (свободное и/или бесплатное ПО); Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО); Notepad ++ (свободное и/или бесплатное ПО); Справочно-правовая система Гарант (лицензионное ПО); 7-zip (свободное и/или бесплатное ПО); Matlab (лицензионное ПО); Visual Studio Code (свободное и/или бесплатное ПО); Apache Spark (свободное и/или бесплатное ПО); PostgreSql (свободное и/или бесплатное ПО), Anylogic (свободное и/или бесплатное ПО), 1С:Предприятие 8.3 (лицензионное ПО).

Учебная аудитория для проведения *лекционных и практических занятий*, лабораторных работ, *организации самостоятельной работы*, проведения текущей и промежуточной аттестаций: специализированная мебель, персональные компьютеры для индивидуальной работы с возможностью подключения к сети «Интернет», мультимедийное оборудование

(проектор, экран, средства звуковоспроизведения).

ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office), специализированное ПО по тематике дисциплины (допускается демоверсия или виртуальный аналог ПО), Intellij IDEA Community Edition (свободное и/или бесплатное ПО); Jet Brains PyCharm Community Edition (свободное и/или бесплатное ПО); Anaconda (свободное и/или бесплатное ПО); Maxima (свободное и/или бесплатное ПО); Scilab (свободное и/или бесплатное ПО); NetBeans IDE (свободное и/или бесплатное ПО); Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО); Notepad ++ (свободное и/или бесплатное ПО); Справочно-правовая система Гарант (лицензионное ПО); 7-zip (свободное и/или бесплатное ПО); Matlab (лицензионное ПО); Visual Studio Code (свободное и/или бесплатное ПО); Apache Spark (свободное и/или бесплатное ПО); PostgreSql (свободное и/или бесплатное ПО), Anylogic (свободное и/или бесплатное ПО).

1) Учебный стенд "Программные средства криптографии", SCRYPTO (страна изготовитель – Россия).

2) Учебно-практический стенд «Системы контроля и управления доступом», ФЗИ-СКУД (страна изготовитель – Россия).

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Стандарты информационной безопасности	ОПК-6	ОПК-6.1	устный опрос, тест, практическая работа
			ОПК-6.2	
			ОПК-6.3	
			ОПК-6.4	
			ОПК-6.10	
		ОПК-8	ОПК-8.10	
		ОПК-11	ОПК-11.4	
2	Формальные модели безопасности компьютерных систем	ОПК-6	ОПК-6.5	устный опрос, тест, практическая работа
			ОПК-6.6	
			ОПК-6.9	
		ОПК-8	ОПК-8.10	
		ОПК-11	ОПК-11.1	
			ОПК-11.2	
			ОПК-11.3	
			ОПК-11.4	
			ОПК-11.5	
3	Методы и средства обоснования требований и оценки защищенности компьютерных систем	ОПК-6	ОПК-6.5	устный опрос, тест, практическая работа
			ОПК-6.6	
			ОПК-6.7	
			ОПК-6.8	
			ОПК-6.9	
			ОПК-6.10	
		ОПК-8	ОПК-8.10	
			ОПК-8.11	
		ОПК-11	ОПК-11.2.	
Промежуточная аттестация, форма контроля - экзамен				Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

– практические работы.

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

Технология проведения

Все практические работы обязательны для выполнения. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания

– оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания, и они правильные, даны пояснения);

– оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к экзамену.

Перечень вопросов к экзамену (КИМ №1)

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.

Критерии оценки ответов на вопросы экзамена

Для оценивания результатов обучения на экзамене используется – 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии

оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.
Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле (При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». Приэтом, все практические работы должны быть выполнены и защищены

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все практические работы должны быть выполнены и защищены.

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):

В1

Мощность какого множества модели ХРУ больше: субъектов или объектов ?			*МС*
		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. (МС/МА)			

В10

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**
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**
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) <u>открытые задания (тестовые, средний уровень сложности):</u>

К1

Сколько примитивных (элементарных) операций используется в классической модели ХРУ?			*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.*			

К2

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**
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 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.	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 XPY?			*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?			*МС*
		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. (МС/МА)			

B21

Сколько функций уровня безопасности используется в модели безопасности переходов?			*МС*
		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. (МС/МА)			

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

К4

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** o (создание нового объекта o) 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**
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**
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**
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 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.			

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).