ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказом ректора
от «02» июня 2023 г. № 424-1

Б1.О.62 Моделирование процессов и систем защиты информации

рабочая программа дисциплины

Специальность/направление подготовки – 10.05.03 Информационная безопасность автоматизированных систем
Специализация/профиль – Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – очная форма 5 лет, 6 месяцев
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 4
Часов по учебному плану (УП) – 144

Формы промежуточной аттестации
очная форма обучения:
зачет 10 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	10	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	85	**85**
– лекции	34	**34**
– практические (семинарские)	51	**51**
– лабораторные		
Самостоятельная работа	59	**59**
Итого	144	**144**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем утвержденным Приказом Минобрнауки России от от 26.11.2020 № 1457.

Программу составил(и):
К.э.н., доцент, заведующий кафедрой, Т. К. Кириллова

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «2» июня 2023 г. № 12

Зав. кафедрой, к.э.н. , доцент Т.К. Кириллова

1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цель дисциплины

1	ознакомление с современными основами построения математических моделей сложных информационных процессов и систем защиты информации

1.2 Задачи дисциплины

1	ознакомить обучающихся со способами формулирования проблемы моделирования процессов и систем защиты информации;
2	ознакомить с процессами сбора, передачи и накопления при моделировании процессов и систем защиты информации;
3	ознакомить с подходами к оцениванию защищенности и обеспечения информационной безопасности компьютерных систем

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.
Цель достигается по мере решения в единстве следующих задач:
– формирование сознательного отношения к выбранной профессии;
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;
– формирование психологии профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть

2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины

1	Б1.О.07 Математический анализ
2	Б1.О.08 Алгебра и геометрия
3	Б1.О.09 Дискретная математика
4	Б1.О.10 Математическая логика и теория алгоритмов
5	Б1.О.11 Теория вероятностей и математическая статистика
6	Б1.О.12 Численные методы и теория оптимизации
7	Б1.О.25 Теория информации
8	Б1.О.27 Основы кибернетики
9	Б1.О.31 Безопасность сетей ЭВМ
10	Б1.О.36 Сети и системы передачи информации
11	Б1.О.37 Защита информации от утечки по техническим каналам
12	Б1.О.39 Программно-аппаратные средства защиты информации
13	Б1.О.42 Открытые информационные системы
14	Б1.О.45 Виртуальные частные сети
15	Б1.О.47 Информационные технологии
16	Б1.О.51 Кибербезопасность
17	Б1.О.55 Защита объектов критической информационной инфраструктуры

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
2	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-3 Способен использовать математические методы, необходимые для	ОПК-3.1 Знает и имеет навыки применения основ математического анализа, алгебры, теории вероятностей и	Знать: основы математического анализа, алгебры, теории вероятностей и математической статистики, дискретной математики, математической логики и теории алгоритмов, теории автоматов и формальных языков
		Уметь: применять основы математического анализа,

решения задач профессиональной деятельности	математической статистики, дискретной математики, математической логики и теории алгоритмов, теории автоматов и формальных языков	алгебры, теории вероятностей и математической статистики, дискретной математики, математической логики и теории алгоритмов, теории автоматов и формальных языков
		Владеть: навыками применения основ математического анализа, алгебры, теории вероятностей и математической статистики, дискретной математики, математической логики и теории алгоритмов, теории автоматов и формальных языков
	ОПК-3.2 Умеет использовать типовые математические методы и модели для решения задач профессиональной деятельности	Знать: типовые математические методы и модели для решения задач профессиональной деятельности
		Уметь: использовать типовые математические методы и модели для решения задач профессиональной деятельности
		Владеть: навыками использования типовых математических методов и моделей для решения задач профессиональной деятельности
	ОПК-3.3 Владеет подходами к решению стандартных математических задач, выполнению расчетов математических величин, применению математических методов обработки экспериментальных данных для решения задач профессиональной деятельности	Знать: подходы к решению стандартных математических задач, выполнению расчетов математических величин, применению математических методов обработки экспериментальных данных для решения задач профессиональной деятельности
		Уметь: решать стандартные математические задачи, выполнять расчеты математических величин, применять математические методы обработки экспериментальных данных для решения задач профессиональной деятельности
		Владеть: подходами к решению стандартных математических задач, выполнению расчетов математических величин, применению математических методов обработки экспериментальных данных для решения задач профессиональной деятельности
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1 Проводит анализ профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных	Знать: методы анализа профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных
		Уметь: проводить анализ профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных
		Владеть: методами анализа профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных
	ОПК-9.2 Знает основные информационные технологии, используемые в автоматизированных системах, их состояние и тенденции развития	Знать: основные информационные технологии, используемые в автоматизированных системах, их состояние и тенденции развития
		Уметь: применять основные информационные технологии, используемые в автоматизированных системах, их состояние и тенденции развития
		Владеть: основными информационными технологиями, используемые в автоматизированных системах, их состояние и тенденции развития
	ОПК-9.3 Знает текущее состояние и тенденции развития сетей и систем передачи информации	Знать: текущее состояние и тенденции развития сетей и систем передачи информации
		Уметь: найти информацию о текущем состоянии и тенденциях развития сетей и систем передачи информации
		Владеть: информацией о текущем состоянии и тенденциях развития сетей и систем передачи информации

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Системный подход к управлению защитой информации.**						
1.1	Тема 1. Основы теории моделирования.	10	2	4		4	ОПК-3.1 ОПК-3.2
1.2	Тема 2. Выбор уровня описания системы в модели.	10	2	4		4	ОПК-3.3

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
	Алгоритм создания системы комплексной защиты						ОПК-9.1
1.3	Тема 3. Модель формирования множества функций защиты информации.	10		4		6	ОПК-3.1 ОПК-9.1
2.0	**Раздел 2. Метод статистических испытаний.**						
2.1	Тема 4. Алгоритм получения нормально-распределенной случайной величины. Алгоритм получения случайной величины, распределенной по Пуассону. Условия применения пуассоновских процессов для моделирования атак	10	2	4		2	ОПК-3.1 ОПК-3.3
2.2	Тема 5. Модели выбора рационального варианта средства защиты информации на основе экспертной информации	10	4	2		6	ОПК-3.3 ОПК-9.1
2.3	Тема 6. Вероятностная модель системы контроля доступа	10	2	6		4	ОПК-3.3 ОПК-9.1
2.4	Тема 7. Модель на основе нейронных сетей в задачах защиты информации	10	6	6		5	ОПК-3.1 ОПК-9.1 ОПК-9.2
2.5	Тема 8. Программная реализация конечно-автоматной модели	10	2	4		6	ОПК-3.2 ОПК-9.2
3.0	**Раздел 3. Методы моделирования задач информационной безопасности (ИБ).**						
3.1	Тема 9. Модель представления информации с учетом надежности программно-аппаратных средств	10	2	4		4	ОПК-3.1 ОПК-9.2
3.2	Тема 10. Модель процессов обработки запросов системы.	10	4	3		4	ОПК-9.1 ОПК-9.2 ОПК-9.3
3.3	Тема 11. Модель процессов контроля информации, вероятностная модель контроля доступа	10	4	4		6	ОПК-9.1 ОПК-9.3
3.4	Тема 12. Модель процессов воздействия компьютерных вирусов	10	4	2		4	ОПК-9.3
3.5	Тема 13. Модель процессов НСД к информации и программным ресурсам	10		4		4	ОПК-9.1 ОПК-9.2
	Форма промежуточной аттестации – зачет	10					
	Итого часов (без учёта часов на промежуточную аттестацию)		34	51		59	

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Математическое моделирование : учебное пособие / . пос. Караваево : КГСХА, 2021. - 76с. - Текст: электронный. - URL: https://e.lanbook.com/book/252131 (дата обращения: 19.04.2023)	Онлайн
6.1.1.2	Ададуров, С. Е. Методология и система обеспечения информационной безопасности на железнодорожном транспорте : учеб. для студентов, обучающихся по специальности 090302.65 "Информационная безопасность телекоммуникационных систем" ВПО : в 2 ч. / С. Е. Ададуров [и др.] ; ред. А.	27

	А. Корниенко. М. : УМЦ по образованию на ж.-д. трансп., 2014. - 439с.	
6.1.1.3	Внуков, А. А. Защита информации : учебное пособие для вузов - 3-е изд. пер. и допА. А. Внуков.. Москва : Юрайт, 2022. - 161с. - Текст: электронный. - URL: https://urait.ru/bcode/490277 (дата обращения: 09.09.2022)	Онлайн
6.1.1.4	Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации : учебное пособие / С. И. Козьминых. Москва : Юнити-Дана, 2020. - 544с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=615695 (дата обращения: 14.09.2022)	Онлайн
6.1.2 Дополнительная литература		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	А. А. Корниенко, М. А. Еремеев, В. Н. Кустов [и др.] ; под редакцией А. А. Корниенко ; рецензенты : Д. Д. Иванов, В. Ю. Горелик Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте : в 2 частях : учебник / А. А. Корниенко, М. А. Еремеев, В. Н. Кустов [и др.] ; под редакцией А. А. Корниенко ; рецензенты : Д. Д. Иванов, В. Ю. Горелик. Москва : УМЦ ЖДТ, - 448с. - Текст: электронный. - URL: https://umczdt.ru/books/42/30051/	Онлайн
6.1.2.2	Алекперов, И. Д. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания : учебное пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. Ростов-на-Дону : ИУБиП, 2020. - 114с. - Текст: электронный. - URL: https://e.lanbook.com/book/248747 (дата обращения: 19.04.2023)	Онлайн
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Кириллова, Т.К. Методические указания по изучению дисциплины Б1.О.62 Моделирование процессов и систем защиты информации по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Безопасность открытых информационных систем / Т. К. Кириллова; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 13 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_8238_1529_2023_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Научная электронная библиотека «КиберЛенинка» — https://cyberleninka.ru/	
6.2.2	Научная электронная библиотека eLIBRARY.RU — https://elibrary.ru/	
6.2.3	Электронная библиотека Учебно-методического центра по образованию на железнодорожном транспорте «ЭБ УМЦ ЖДТ» — https://umczdt.ru/books/	
6.2.4	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.2.5	Электронно-библиотечная система «Образовательная платформа ЮРАЙТ», https://urait.ru/	
6.2.6	Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/	
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/	
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	Не предусмотрено	
6.3.3 Информационные справочные системы		
6.3.3.1	Не предусмотрены	
6.4 Правовые и нормативные документы		
6.4.1	Не предусмотрены	

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	
1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	
Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Самостоятельная работа	Обучение по дисциплине «Моделирование процессов и систем защиты информации» предусматривает активную самостоятельную работу обучающегося. В

	разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией ИрГУПС, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций, в формировании которых участвует дисциплина.
Программа контрольно-оценочных мероприятий.
Показатели оценивания компетенций, критерии оценки

Дисциплина «Моделирование процессов и систем защиты информации» участвует в формировании компетенций:

ОПК-3. Способен использовать математические методы, необходимые для решения задач профессиональной деятельности

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
10 семестр				
1.0	**Раздел 1. Системный подход к управлению защитой информации**			
1.1	Текущий контроль	Тема 1. Основы теории моделирования.	ОПК-3.1 ОПК-3.2	Собеседование (устно)
1.2	Текущий контроль	Тема 2. Выбор уровня описания системы в модели. Алгоритм создания системы комплексной защиты	ОПК-3.3 ОПК-9.1	Собеседование (устно)
1.3	Текущий контроль	Тема 3. Модель формирования множества функций защиты информации.	ОПК-3.1 ОПК-9.1	Доклад (устно)
2.0	**Раздел 2. Метод статистических испытаний**			
2.1	Текущий контроль	Тема 4. Алгоритм получения нормально-распределенной случайной величины. Алгоритм получения случайной величины, распределенной по Пуассону. Условия применения пуассоновских процессов для моделирования атак	ОПК-3.1 ОПК-3.3	Доклад (устно)
2.2	Текущий контроль	Тема 5. Модели выбора рационального варианта средства защиты информации на основе экспертной информации	ОПК-3.3 ОПК-9.1	Собеседование (устно)
2.3	Текущий контроль	Тема 6. Вероятностная модель системы контроля доступа	ОПК-3.3 ОПК-9.1	Собеседование (устно)
2.4	Текущий контроль	Тема 7. Модель на основе нейронных сетей в задачах защиты информации	ОПК-3.1 ОПК-9.1 ОПК-9.2	Доклад (устно)
2.5	Текущий контроль	Тема 8. Программная реализация конечно-автоматной модели	ОПК-3.2 ОПК-9.2	Собеседование (устно)
3.0	**Раздел 3. Методы моделирования задач информационной безопасности (ИБ)**			
3.1	Текущий контроль	Тема 9. Модель представления информации с учетом надежности программно-аппаратных средств	ОПК-3.1 ОПК-9.2	Собеседование (устно)
3.2	Текущий контроль	Тема 10. Модель процессов обработки запросов системы.	ОПК-9.1 ОПК-9.2 ОПК-9.3	Доклад (устно)
3.3	Текущий контроль	Тема 11. Модель процессов контроля информации, вероятностная модель контроля доступа	ОПК-9.1 ОПК-9.3	Собеседование (устно)
3.4	Текущий	Тема 12. Модель процессов	ОПК-9.3	Доклад (устно)

	контроль	воздействия компьютерных вирусов		
3.5	Текущий контроль	Тема 13. Модель процессов НСД к информации и программным ресурсам	ОПК-9.1 ОПК-9.2	Собеседование (устно)
	Промежуточная аттестация	Раздел 1. Системный подход к управлению защитой информации. Раздел 2. Метод статистических испытаний. Раздел 3. Методы моделирования задач информационной безопасности (ИБ).		Зачет (собеседование) Зачет - тестирование (компьютерные технологии)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице.

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
2	Доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Зачет	Средство, позволяющее оценить знания, умения, навыков	Перечень

		и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	теоретических вопросов и практических заданий к зачету
2	Тест – промежуточная аттестация в форме зачета	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Тест – промежуточная аттестация в форме зачета

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся верно ответил на 70 % и более тестовых заданий при прохождении тестирования
«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»		Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»		Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	«не зачтено»	Не было попытки выполнить задание

Доклад

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»		Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»		Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	«не зачтено»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль доклада не передана

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1 Типовые контрольные задания для проведения собеседования

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования
«Основы теории моделирования. Основные термины и определения. Классификация методов моделирования Методология разработки моделей»

1. Что такое моделирование и какие цели оно может иметь в различных областях?
2. Какие основные термины и определения, связанные с моделированием вы знаете?

3. Какие виды моделей вы можете перечислить? Назовите их основные характеристики.
4. Что такое эмпирическое моделирование и как оно отличается от математического моделирования?
5. Какие этапы включает в себя методология разработки моделей?

Образец типового варианта вопросов для проведения собеседования
«Выбор уровня описания системы в модели. Алгоритм создания системы комплексной защиты»

1. Какие уровни описания системы в модели вы можете выделить и как они взаимодействуют при создании системы комплексной защиты?
2. Какие основные этапы включает в себя алгоритм создания системы комплексной защиты, начиная с анализа угроз?
3. Какие факторы следует учитывать при выборе уровня описания системы в модели для обеспечения эффективной защиты?
4. Какие методы и инструменты можно использовать для оценки уровня угроз и уязвимостей в системе?
5. Какие принципы комплексной защиты информации считаются наиболее важными и почему?

Образец типового варианта вопросов для проведения собеседования
«Модели выбора рационального варианта средства защиты информации на основе экспертной информации»

1. Что такое модель выбора рационального варианта средства защиты информации и какие задачи она решает?
2. Какие методы экспертной оценки можно использовать при создании такой модели?
3. Какие критерии и параметры обычно учитываются при выборе средства защиты на основе экспертной информации?
4. Какие ограничения могут возникнуть при использовании экспертных данных для принятия решений о защите информации?
5. Можете привести пример применения модели выбора рационального средства защиты информации в практике?

Образец типового варианта вопросов для проведения собеседования
«Вероятностная модель системы контроля доступа»

1. Что представляет собой вероятностная модель системы контроля доступа?
2. Какие основные компоненты включает в себя такая модель?
3. Какие преимущества и недостатки могут быть связаны с использованием вероятностных моделей в системах контроля доступа?
4. Какие вероятностные методы могут использоваться для анализа и улучшения системы контроля доступа?
5. Какие факторы могут повлиять на точность и надежность вероятностной модели?

Образец типового варианта вопросов для проведения собеседования
«Программная реализация конечно-автоматной модели»

1. Что такое конечно-автоматная модель и какие задачи она может решать в программной реализации?
2. Какие основные компоненты включает в себя конечно-автоматная модель?
3. Какие языки программирования и инструменты часто используются при реализации таких моделей?
4. Какие сценарии и примеры использования конечно-автоматных моделей в программировании вы можете привести?
5. Как обеспечить надежность и безопасность программной реализации конечно-автоматной модели?

Образец типового варианта вопросов для проведения собеседования

«Модель представления информации с учетом надежности программно-аппаратных средств»
1. Что означает модель представления информации с учетом надежности программно-аппаратных средств?
2. Какие факторы и параметры обычно учитываются при создании такой модели?
3. Какие методы оценки надежности программных и аппаратных средств могут быть использованы в такой модели?
4. Какие применения могут быть у моделей представления информации с учетом надежности?
5. Какие технологии и инструменты помогают реализовать такие модели в практике?

Образец типового варианта вопросов для проведения собеседования
«Модель процессов контроля информации, вероятностная модель контроля доступа»
1. Что представляют собой модель процессов контроля информации и вероятностная модель контроля доступа?
2. Какие основные этапы включают в себя эти модели при обеспечении безопасности информации?
3. Какие принципы вероятностного контроля доступа могут быть применены в системах?
4. Какие риски и угрозы они помогают уменьшить или предотвратить?
5. Какие методы и технологии могут использоваться для анализа и улучшения таких моделей в системах контроля информации?

Образец типового варианта вопросов для проведения собеседования
«Модель процессов НСД к информации и программным ресурсам»
1. Что включает в себя модель процессов НСД к информации и программным ресурсам?
2. Какие основные задачи и функции такой модели решает?
3. Какие методы и алгоритмы могут быть использованы при ее создании?
4. Каким образом модель процессов НСД помогает управлять доступом к информации и программным ресурсам?
5. Какие факторы и требования безопасности следует учитывать при реализации такой модели?

3.2 Типовые контрольные темы для написания докладов

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов тем для написания докладов.

Образец тем докладов
«Модель формирования множества функций защиты информации. Расчет вероятности нахождения системы в состоянии «защита обеспечена». Расчет вероятности нахождения системы в состоянии «защита нарушена»»
1. Исследование методов формирования функций защиты информации.
2. Анализ вероятности нарушения системы защиты информации при известных функциях защиты.
3. Оценка эффективности системы защиты информации на основе моделирования.
4. Сравнительный анализ методов расчета вероятности нарушения системы защиты.
5. Практические аспекты применения модели формирования функций защиты информации.

Образец тем докладов
«Алгоритм получения нормально-распределенной случайной величины. Алгоритм получения случайной величины, распределенной по Пуассону. Условия применения пуассоновских процессов для моделирования атак»
1. Методы генерации случайных данных с нормальным распределением.
2. Алгоритмы генерации случайных величин, следующих закону Пуассона.
3. Применение пуассоновских процессов в задачах моделирования атак на информационные системы.

4. Сравнение различных методов моделирования случайных событий.
5. Анализ применимости алгоритмов генерации случайных данных в задачах кибербезопасности.

Образец тем докладов

«Модель на основе нейронных сетей в задачах защиты информации»

1. Исследование использования нейронных сетей для обнаружения аномалий в сетевом трафике.
2. Анализ применения нейронных сетей в системах обнаружения вторжений.
3. Разработка нейронных моделей для определения вредоносных программ.
4. Сравнение эффективности нейронных сетей и традиционных методов в области кибербезопасности.
5. Применение глубокого обучения в моделировании и обеспечении безопасности информации.

Образец тем докладов

«Модель процессов обработки запросов системы. Модель процессов сбора обновлений информации от источников»

1. Анализ процессов обработки запросов в информационных системах.
2. Моделирование процессов сбора данных и информационной агрегации.
3. Оптимизация процессов обработки больших объемов данных.
4. Применение технологий распределенных систем в моделировании процессов сбора информации.
5. Автоматизация процессов обработки запросов и обновлений в реальном времени.

Образец тем докладов

«Модель процессов воздействия компьютерных вирусов»

1. Исследование механизмов распространения компьютерных вирусов.
2. Моделирование жизненного цикла вредоносных программ.
3. Анализ методов защиты от компьютерных вирусов и антивирусных стратегий.
4. Оценка воздействия компьютерных вирусов на информационные системы и данные.
5. Тенденции в развитии вирусных атак и перспективы в области кибербезопасности.

3.3 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-3.1 ОПК-3.2	Основы теории моделирования. Основные термины и определения. Классификация методов моделирования Методология разработки моделей	Знание	4 – ОТЗ 4 – ЗТЗ
ОПК-9.1	Выбор уровня описания системы в модели. Алгоритм создания системы комплексной защиты	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1	Модель формирования множества функций защиты информации. Расчет вероятности нахождения системы в состоянии «защита обеспечена». Расчет вероятности нахождения системы в состоянии «защита нарушена»	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-3.1	Алгоритм получения нормально-распределенной случайной	Знание	4 – ОТЗ

ОПК-3.3	величины. Алгоритм получения случайной величины, распределенной по Пуассону. Условия применения пуассоновских процессов для моделирования атак		4 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-3.3	Модели выбора рационального варианта средства защиты информации на основе экспертной информации	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1	Вероятностная модель системы контроля доступа	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1 ОПК-9.2	Модель на основе нейронных сетей в задачах защиты информации	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-9.2	Программная реализация конечно-автоматной модели	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-3.1	Модель представления информации с учетом надежности программно-аппаратных средств	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1 ОПК-9.2	Модель процессов обработки запросов системы. Модель процессов сбора обновлений информации от источников	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-9.1 ОПК-9.3	Модель процессов контроля информации, вероятностная модель контроля доступа	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-9.3	Модель процессов воздействия компьютерных вирусов	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-9.2	Модель процессов НСД к информации и программным ресурсам	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Итого	50 – ОТЗ 50 – ЗТЗ

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

1. Последовательность этапов моделирования:

а) цель, объект, модель, метод, алгоритм, программа, эксперимент, анализ, уточнение

б) объект, цель, модель, эксперимент, программа, анализ, тестирование

в) цель, модель, объект, алгоритм, программа, эксперимент, уточнение выбора объекта

2. Совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации в автоматизированных системах обработки данных – это

а) техническая система защиты информации;

б) программно-аппаратная система защиты информации;

в) комплексная система защиты информации.

3. Как называется модель нарушителя, которая представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, характеризующих результаты действий, и функциональных зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами объекта и системы охраны?

а) количественная
б) математическая
в) косвенная
г) содержательная

4.Принцип однородности памяти Фон-Неймана означает:
а) Программы и данные хранятся в одной и той же памяти
б) Все ячейки памяти выполнены из одинаковых элементов
в) Под данные и команды отводятся строго одинаковые объемы памяти

5. Этап моделирования предполагающий выбор уровня описания системы –
а) алгоритм
б) анализа угроз
в) программа

6. Что такое множество весовых значений нейрона? (два и более варианта)
а) множество значений, характеризующих "силу" соединений данного нейрона с нейронами предыдущего слоя
б) множество значений, характеризующих "силу" соединений данного нейрона с нейронами последующего слоя
в) множество значений, моделирующих "силу" биологических синоптических связей
г) множество значений, характеризующих вычислительную "силу" нейрона

7. Какое из вариантов обеспечивает точность, безошибочность и защиту изменения информации организации?
а) Доступность
б) Целостность
в) Отчетность

8. Необходимым, но не достаточным при определении вируса является такое свойство, как
а) способность к созданию собственных копий
б) наличие механизма, обеспечивающего удаление создаваемых копий
в) использование апробированного математического аппарата.

9. В каких случаях используется метод Монте-Карло?
а) исследуется система, функционирование которой определяется многими вероятностными параметрами элементарных явлений;
б) определение точной погрешности;
в) Высокая сходимость

10. Как называется система безопасности, которая должна иметь по крайней мере одно средство, обеспечивающее безопасность любого потенциального канала утечки информации?
- Правильный ответ: модель системы безопасности с полным перекрытием

11. В типовой системе обнаружения атак основным элементом является
- Правильный ответ: подсистема обнаружения атак

12. Группу из нескольких слоев нейронов, соединенных синапсами, которые работают вместе для обработки данных.
- Правильный ответ: многослойная нейронная сеть

13.Формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей и ответных мер

- Правильный ответ: математическая модель

14. Модель системы контроля доступа к информации основанная на вероятностных распределениях и оценках вероятности различных событий

- Правильный ответ: вероятностная модель системы контроля доступа

15. Какие задачи защиты информации можно решать с помощью моделей на основе нейронных сетей?

- Правильный ответ: Модели на основе нейронных сетей могут использоваться для обнаружения аномалий, классификации угроз, и анализа поведения пользователей в системах защиты информации.

16. Методы сэмплирования и оптимизации параметров модели характерны для

- Правильный ответ: понижения дисперсии

17. Какие факторы следует учитывать при выборе средства защиты информации на основе экспертной информации?

- Правильный ответ: степень угрозы, бюджет, сложность реализации и опыт экспертов

18. Для чего используется анализ угроз, оценка активов, выбор соответствующих контрмер, оценку их эффективности?

- Правильный ответ: Выбора рационального средства защиты информации

3.4 Перечень теоретических вопросов к зачету

(для оценки знаний)

Раздел 1. Системный подход к управлению защитой информации.

1. Основы теории моделирования. Основные термины и определения. Классификация методов моделирования.
2. Принципы системного подхода в моделировании.
3. Виды показателей эффективности. Метод обобщенного показателя. Метод «затраты эффект». Метод целевого программирования.
4. Системный подход к управлению защитой информации. Системные принципы создания комплексной защиты информации.
5. Выбор уровня описания системы в модели. Этапы моделирования.
6. Выбор уровня описания системы в модели. Методология разработки моделей
7. Алгоритм создания системы комплексной защиты.
8. Модель формирования множества функций защиты информации. Расчет вероятности нахождения системы в состоянии «защита обеспечена». Расчет вероятности нахождения системы в состоянии «защита нарушена». Расчет вероятности нахождения системы в состоянии «защита разрушена».

Раздел 2. Метод статистических испытаний.

9. Метод статистических испытаний (метод Монте-Карло).
10. Моделирование случайных факторов. Проверка равномерности и стохастичности.
11. Метод интерпретации. Моделирование непрерывных случайных величин.
12. Модель нарушителя.
13. Моделирование по событиям. Моделирование параллельных процессов.
14. Подбор параметров распределений, реализуемых в моделях.
15. Метод Фон - Неймана.

Раздел 3. Методы моделирования задач информационной безопасности (ИБ).

16. Алгоритм получения нормально-распределенной случайной величины.
17. Алгоритм получения случайной величины, распределенной по Пуассону.
18. Условия применения пуассоновских процессов для моделирования атак.

19. Модели выбора рационального варианта средства защиты информации на основе экспертной информации.

20. Вероятностная модель системы контроля доступа к информации.

21. Модель на основе нейронных сетей в задачах защиты информации.

22. Стратегическое планирование имитационного экспериментов.

23. Тактическое планирование имитационного экспериментов. Методы понижения дисперсии.

24. Оценка качества имитационной модели. Методы оценки адекватности.

25. Методы оценки устойчивости модели.

26. Методы оценки чувствительности модели.

27. Калибровка модели.

28. Оценка влияния и взаимосвязи факторов. Однофакторный и дисперсионный анализ.

3.5 Перечень типовых простых практических заданий к зачету

(для оценки умений)

1. Разработать сценарий действий нарушителя информационной безопасности указанной преподавателем организации с использованием сети Петри;
2. Определить показатели защищенности информации при несанкционированном доступе указанной преподавателем организации;
3. Применить методологию и стандарты IDEF для моделирования процессов в системе защиты информации указанной преподавателем организации;
4. Применить методики анализа рисков информационной безопасности указанной преподавателем организации для малого и среднего бизнеса;
5. Сделать анализ рисков информационной безопасности с использованием нечеткой логики указанной преподавателем организации.

3.6 Перечень типовых практических заданий к зачету

(для оценки навыков и (или) опыта деятельности)

1. Разработать план реагирования на инциденты информационной безопасности для фиктивной компании. Включите в него этапы обнаружения, анализа и реагирования на различные типы инцидентов;
2. Провести аудит безопасности в компании, выявив уязвимости и рекомендации по их устранению. Создайте подробный отчет об аудите с описанием найденных проблем и рекомендациями;
3. Разработать политику информационной безопасности для организации, включая правила паролей, управление доступом и процедуры обработки конфиденциальных данных;
4. Смоделировать сценарий атаки на внутреннюю сеть организации с использованием программ для тестирования на проникновение. Опишите обнаруженные уязвимости и предложите меры по их устранению;
5. Провести анализ рисков информационной безопасности с использованием методов нечеткой логики. Определите вероятность и воздействие различных угроз на организацию, а также разработайте план действий для управления этими рисками.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения

средства	
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Доклад	Защита докладов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему докладов и требования, предъявляемые к их выполнению и защите

Для организации и проведения промежуточной аттестации составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Перечень теоретических вопросов и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Шкала оценивания
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.