ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «31» мая 2024 г. № 425-1

Б1.О.13 Управление информационной безопасностью автоматизированных систем

рабочая программа дисциплины

Специальность/направление подготовки – 10.04.01 Информационная безопасность
Специализация/профиль – Безопасность информационных систем и технологий
Квалификация выпускника – Магистр
Форма и срок обучения – очная форма 2 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 5
Часов по учебному плану (УП) – 180

Формы промежуточной аттестации
очная форма обучения:
зачет 1 семестр, экзамен 2 семестр

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

Семестр	1	2	**Итого**
Вид занятий	Часов по УП	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	68	51	**119**
– лекции	34	17	**51**
– практические (семинарские)	34	34	**68**
– лабораторные			
Самостоятельная работа	4	21	**25**
Экзамен		36	**36**
Итого	72	108	**180**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 26.11.2020 № 1455.

Программу составил(и):
к.э.н., доцент, Н.И.Глухов

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «21» мая 2024 г. № 11

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

1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цель дисциплины	
1	применения практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии
1.2 Задачи дисциплины	
1	приобретение необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность
2	формирование у обучаемых целостного представления об организации и сущности процессов управления информационной безопасностью (ИБ) на предприятии как результата внедрения системного подхода по решению задач обеспечения ИБ

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	ФТД.01 Интеллектуальные информационные системы
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.11 Экономика и управление
2	Б2.О.02(Н) Производственная - научно-исследовательская работа
3	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
4	Б3.02(Д) Защита выпускной квалификационной работы
5	ФТД.02 Корпоративные информационные системы

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-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.1 Знает основные направления и тенденции развития технологий в области ИБ	Знать: основные направления и тенденции развития технологий в области ИБ
		Уметь: разрабатывать планы и программы по основным направлениям и тенденциям развития технологий в области ИБ
		Владеть: навыками по основным направлениям и тенденциям развития технологий в области ИБ
	ОПК-4.2 Умеет осуществлять сбор, обработку и анализ современной научно-технической информации в области информационной безопасности, умеет использовать эти знания в при решении поставленных задач	Знать: методы сбора, обработки и анализа научно-технической информации
		Уметь: разрабатывать планы и программы проведения научных исследований и технических разработок
		Владеть: навыками работ по сбору, обработке и анализу научно-технической информации по теме исследования

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. Система управления информационной безопасностью**						
1.1	Тема 1. Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии информационных ресурсов и защиты информации	1	12			1	ОПК-4.1 ОПК-4.2
1.2	Тема 2. Политика безопасности	1		8		2	ОПК-4.1 ОПК-4.2
1.3	Тема 3. Аудит информационной безопасности	1		6		2	ОПК-4.1

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
							ОПК-4.2
1.4	Тема 4. Организация обеспечения информационной безопасности автоматизированных систем	1		8		2	ОПК-4.1 ОПК-4.2
1.5	Тема 5. Средства поддержки процессов управления информационной безопасностью	1	7			1	ОПК-4.1 ОПК-4.2
2.0	**Раздел 2. Комплексная система защиты информации**						
2.1	Тема 6. Сущность и задачи комплексной системы защиты информации	1		6		2	ОПК-4.1 ОПК-4.2
2.2	Тема 7. Факторы, влияющие на организацию комплексной системы защиты информации	1	8			1	ОПК-4.1 ОПК-4.2
2.3	Тема 8. Определение компонентов комплексной системы защиты информации	1		8		2	ОПК-4.1 ОПК-4.2
2.4	Тема 9. Определение условий функционирования комплексной системы защиты информации	1	10			1	ОПК-4.1 ОПК-4.2
2.5	Тема 10. Разработка модели комплексной системы защиты информации	1		6		2	ОПК-4.1 ОПК-4.2
2.6	Тема 11. Технологическое и организационное построение комплексной системы защиты	1	8			1	ОПК-4.1 ОПК-4.2
	Форма промежуточной аттестации – зачет	1					
3.0	**Раздел 3. Управление комплексной системой защиты информации**						
3.1	Тема 12. Назначение, структура и содержание управления комплексной системой защиты информации	2		6		2	ОПК-4.1 ОПК-4.2
3.2	Тема 13. Принципы и методы планирования комплексной системы защиты информации	2		6		2	ОПК-4.1 ОПК-4.2
3.3	Тема 14. Сущность и содержание контроля функционирования комплексной системы защиты информации	2		8		2	ОПК-4.1 ОПК-4.2
3.4	Тема 15. Общая характеристика подходов к оценке эффективности систем защиты информации	2	6			1	ОПК-4.1 ОПК-4.2
3.5	Тема 16. Методы и модели оценки эффективности комплексной системы защиты информации	2		6		1	ОПК-4.1 ОПК-4.2
	Форма промежуточной аттестации – экзамен	2	36				ОПК-4.1 ОПК-4.2
	Итого часов (без учёта часов на промежуточную аттестацию)		51	68		25	

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	Краковский, Ю. М. Информационная безопасность и защита информации : учеб. пособие / Ю. М. Краковский ; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ. — Иркутск : ИрГУПС, 2016. — 224 с. — Текст : непосредственный.	95
6.1.1.2	Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. — Москва, Берлин	Онлайн

	: Директ-Медиа, 2015. — 255 с. — URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 18.04.2024). — Текст : электронный.	
6.1.1.3	Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. — Самара : Самарский государственный архитектурно-строительный университет, 2014. — 113 с. — URL: https://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.2 Дополнительная литература		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 324 с. — URL: https://e.lanbook.com/book/370967 (дата обращения: 15.04.2024). — Текст : электронный.	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	Глухов Н.И. Методические указания по изучению дисциплины Б1.0.13 Управление информационной безопасностью автоматизированных систем по направлению подготовки 10.04.01 Информационная безопасность автоматизированных систем, профиль «Безопасность информационных систем и технологий» / Н.И. Глухов ; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 11 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47499_1506_2024_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.2.2	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-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)
3	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 «Управление информационной безопасностью автоматизированных систем» 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 «Управление информационной безопасностью автоматизированных систем» участвует в формировании компетенций:

ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
1 семестр				
1.0	**Раздел 1. Система управления информационной безопасностью**			
1.1	Текущий контроль	Тема 1. Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии информационных ресурсов и защиты информации	ОПК-4.1 ОПК-4.2	Собеседование (устно)
1.2	Текущий контроль	Тема 2. Политика безопасности	ОПК-4.1 ОПК-4.2	Собеседование (устно)
1.3	Текущий контроль	Тема 3. Аудит информационной безопасности	ОПК-4.1 ОПК-4.2	Собеседование (устно)
1.4	Текущий контроль	Тема 4. Организация обеспечения информационной безопасности автоматизированных систем	ОПК-4.1 ОПК-4.2	Собеседование (устно)
1.5	Текущий контроль	Тема 5. Средства поддержки процессов управления информационной безопасностью	ОПК-4.1 ОПК-4.2	Собеседование (устно)
2.0	**Раздел 2. Комплексная система защиты информации**			
2.1	Текущий контроль	Тема 6. Сущность и задачи комплексной системы защиты информации	ОПК-4.1 ОПК-4.2	Собеседование (устно)
2.2	Текущий контроль	Тема 7. Факторы, влияющие на организацию комплексной системы защиты информации	ОПК-4.1 ОПК-4.2	Собеседование (устно)
2.3	Текущий контроль	Тема 8. Определение компонентов комплексной системы защиты информации	ОПК-4.1 ОПК-4.2	Собеседование (устно)
2.4	Текущий контроль	Тема 9. Определение условий функционирования комплексной системы защиты информации	ОПК-4.1 ОПК-4.2	Собеседование (устно)
2.5	Текущий контроль	Тема 10. Разработка модели комплексной системы защиты информации	ОПК-4.1 ОПК-4.2	Собеседование (устно)
2.6	Текущий контроль	Тема 11. Технологическое и организационное построение комплексной системы защиты	ОПК-4.1 ОПК-4.2	Собеседование (устно)
	Промежуточная аттестация	Раздел 1. Система управления информационной безопасностью Раздел 2. Комплексная система защиты информации		Зачет (собеседование) Зачет - тестирование (компьютерные технологии)
2 семестр				
3.0	**Раздел 3. Управление комплексной системой защиты информации**			
3.1	Текущий контроль	Тема 12. Назначение, структура и содержание управления	ОПК-4.1 ОПК-4.2	Собеседование (устно)

		комплексной системой защиты информации		
3.2	Текущий контроль	Тема 13. Принципы и методы планирования комплексной системы защиты информации	ОПК-4.1 ОПК-4.2	Собеседование (устно)
3.3	Текущий контроль	Тема 14. Сущность и содержание контроля функционирования комплексной системы защиты информации	ОПК-4.1 ОПК-4.2	Собеседование (устно)
3.4	Текущий контроль	Тема 15. Общая характеристика подходов к оценке эффективности систем защиты информации	ОПК-4.1 ОПК-4.2	Собеседование (устно)
3.5	Текущий контроль	Тема 16. Методы и модели оценки эффективности комплексной системы защиты информации	ОПК-4.1 ОПК-4.2	Собеседование (устно)
	Промежуточная аттестация	Все разделы	ОПК-4.1 ОПК-4.2	Экзамен (собеседование) Экзамен - 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

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС

1	Зачет	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень 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
3	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (образец экзаменационного билета) к экзамену
4	Тест – промежуточная аттестация в форме экзамена	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 и экзамена. Шкала оценивания уровня освоения компетенций

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«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
«хорошо»		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
«удовлетворительно»		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	Минимальный

		неточностей при ответе на дополнительные вопросы	
«неудовлетворительно»	«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 и экзамена

Шкала оценивания		Критерии оценивания
«отлично»	«зачтено»	Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования
«хорошо»		Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования
«удовлетворительно»		Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования
«неудовлетворительно»	«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

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
«Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии информационных ресурсов и защиты информации»

1. Понятие «принятие решений» в широком и узком смысле.
2. Понятие «управленческое решение».

3. Что такое технология разработки решения?
4. Цель, объект и предмет разработки управленческих решений
5. Классификация видов решений.
6. Программируемые и непрограммируемые управленческие решения.
7. Основанные на суждениях, интуитивные и творческие решения.
8. Решения, типичные для общих функций управления
9. Составляющие задачи принятия управленческого решений.
10. Понятие проблемной ситуации.
11. Ограничения и критерии при принятии решения.
12. Схема процесса принятия управленческого решения.
13. Механизм предпочтений лица, принимающего решение.
14. Варианты алгоритмов разработки и принятия решений с учетом проблем и задач, стоящих перед лицами, принимающими решения.
15. Содержание и особенности этапов полного процесса разработки управленческого решения.

Образец типового варианта вопросов для проведения собеседования
«Политика безопасности»

1. Организационно-правовой статус сотрудников информационной безопасности?
2. Порядок доступа пользователей к информационным системам, в которых обрабатывается информация конфиденциального характер?
3. Средства и системы защиты ИС?
4. Локальная безопасность. Антивирусная защита?
5. Защищенные каналы с использованием криптозащиты, на базе решений VipNet, VPN, Банк-клиент или других, сертифицированных ФСТЭК?
6. Разграничение прав доступа к информационным системам и системам хранения данных?
7. Организация физической безопасности
8. Как осуществляется хранение информации конфиденциального характера локально на компьютере?
9. Ответственность за соблюдение положений Политики ИБ?
10. Дублирование, резервное копирование и хранение информации

Образец типового варианта вопросов для проведения собеседования
«Назначение, структура и содержание управления комплексной системой защиты информации»

1. Что такое модель системы безопасности информации?
2. Может ли использоваться моделирование при принятии управленческих решений?
3. Какие типы моделей вы знаете?
4. Обозначьте основные этапы процесса построения модели
5. Какие проблемы моделирования вы можете назвать?
6. Как в практике разработки УР могут применяться модели теории игр?
7. Как в практике разработки УР могут применяться модели управления запасами?
8. Как в практике разработки УР могут применяться модели линейного программирования?
9. В каких ситуациях построение модели невозможно?
10. Выделите преимущества и недостатки методов моделирования.

Образец типового варианта вопросов для проведения собеседования
«Принципы и методы планирования комплексной системы защиты информации»

1. Что понимается под оперативным планированием ИБ? Какие виды планирования существуют в ИБ предприятия?
2. В чем заключается календарное планирование? Что оно предусматривает?

3. Какие системы оперативного планирования применяются? Что представляет собой система планирования ИБ предприятия?

4. В чем сущность позаказной системы? Где она применяется?

5. Как ведется планирование производства по заделам? Какие виды заделов планируются?

6. Какие методы оперативного планирования можно использовать на предприятии? Чем отличается объемный метод от календарного?

7. Что представляет собой объемно-календарный метод планирования? Для каких целей он служит?

8. В чем состоит назначение объемно-динамического метода планирования? Какие показатели он позволяет планировать?

9. Какие объемно-календарные нормативы применяются в планировании? Что служит первичным календарным нормативом?

10. Где применяются нормативы опережений? Как они определяются?

Образец типового варианта вопросов для проведения собеседования
«Методы и модели оценки эффективности комплексной системы защиты информации»

1. С какими проблемами приходится сталкиваться при оценке эффективности управленческих решений?
2. В чём цель процедуры контроля управленческих решений?
3. Какие существуют виды контроля управленческих решений?
4. Каковы основные принципы организации контроля ИБ?
5. Что понимают под ответственностью менеджера за принятое управленческое решение?
6. Блок – схема разработки управленческого решения ИБ.
7. Роль человеческого фактора в процессе принятии управленческих решений.
8. Влияние авторитета на процесс принятия управленческих решений.
9. Влияние паники на подготовку управленческих решений.
10. Условия и факторы качества УР ИБ.
11. Процесс разработки УР в сложных ситуациях.
12. Организация процесса разработки УР ИБ.
13. Методы и технологии выработки УР в условиях определенности.
14. Функции решения в организации процесса управления.
15. Организация вычислительной поддержки управленческой деятельности.
16. Сущность процессов самоорганизации в малой группе при принятии УР
17. Целевая ориентация УР.
18. Основы автоматизации процесса принятия УР.

3.2 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-4.1 ОПК-4.2	Тема 1. Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии информационных ресурсов и защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 2. Политика безопасности	Знание	1 – ОТЗ 1 – ЗТЗ

		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 3. Аудит информационной безопасности	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 4. Организация обеспечения информационной безопасности автоматизированных систем	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 5. Средства поддержки процессов управления информационной безопасностью	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 6. Сущность и задачи комплексной системы защиты информации	Знание	2 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 7. Факторы, влияющие на организацию комплексной системы защиты информации	Знание	2 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 8. Определение компонентов комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 2 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 9. Определение условий функционирования комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 2 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 10. Разработка модели комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 11. Технологическое и организационное построение комплексной системы защиты	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 12. Назначение, структура и содержание управления комплексной системой защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ

ОПК-4.1 ОПК-4.2	Тема 13. Принципы и методы планирования комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 14. Сущность и содержание контроля функционирования комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 15. Общая характеристика подходов к оценке эффективности систем защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-4.1 ОПК-4.2	Тема 16. Методы и модели оценки эффективности комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – 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.

Образец типового варианта итогового теста,
предусмотренного рабочей программой дисциплины

1. Информация – это

Ответ: сведения (сообщения, данные) независимо от формы их представления.

2. Обладатель информации – это

Ответ: лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

3. Выберите правильное определение термина «предоставление информации»:

а) действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

б) действия, направленные на распространение сведений в средствах массовой информации;

в) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

г) действия, направленные на получение информации как определённым, так и неопределённым кругом лиц или передачу информации как определенному, так и неопределённому кругу лиц.

4. Выберите правильное определение термина «защищаемые помещения»:

а) помещения, специально предназначенные для хранения носителей конфиденциальной информации;

б) помещения, специально предназначенные для размещения технических средств информационной системы;

в) помещения, специально предназначенные для хранения носителей конфиденциальной информации и размещения технических средств информационной системы;

г) помещения, специально предназначенные для проведения конфиденциальных мероприятий.

5. К рекомендуемым методам и способам защиты информации в информационных системах относятся (выберите все верные варианты ответов):

а) методы и способы защиты информации от несанкционированного доступа;

б) методы и способы сокрытия информации от внутренних нарушителей;

в) методы и способы устранения конкурентов;

г) методы и способы защиты информации от утечки по техническим каналам.

6. Средствами защиты информации, подлежащими сертификации, являются (выберите все верные варианты ответов):

а) строительные материалы, используемые для отделки помещений, в которых размещаются отдельные элементы АС;

б) детали интерьера, используемые для размещения АИС;

в) средства контроля эффективности применения средств защиты информации;

г) средства контроля эффективности прочности ограждений;

д) средства защиты информации (технические, программные, программно-аппаратные) от НСД, блокировки доступа и нарушения целостности.

7. Технические способы защиты информации в зависимости от используемых средств классифицируются как (выберите все верные варианты ответов):

а) полуактивные;

б) пассивные;

в) разноплановые;

г) удостоверяющие;

д) активные.

8. Технический канал утечки информации – это

Ответ: совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

9. Техническими каналами утечки информации являются (выберите все верные варианты ответов):

а) кражи технических средств информационной системы;

б) утечки акустической (речевой) информации;

в) утечки информации, реализуемые через общедоступные информационные сети;

г) утечки видовой информации;

д) утечки информации по каналам побочных электромагнитных излучений;

е) утечки информации, реализуемые через интернет.

10. Несанкционированный доступ к информации – это

Ответ: доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств.

11. Механизм контроля целостности СЗИ Secret Net предназначен для _____

Ответ: слежения за неизменностью содержимого ресурсов компьютера.

12. Механизм замкнутой программной среды СЗИ Secret Net и Dallas Lock предназначен для

а) ограничения использования программного обеспечения на компьютере;

б) установки ограниченного количества программ;

в) сбора сведений об используемых приложениях.

13. В СЗИ Secret Net пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями

а) «конфиденциально»;

б) «секретно»;

в) «строго конфиденциально»,

г) «неконфиденциально».

14. К какому типу криптосистем относится алгоритм AES?

а) несимметричные;

б) асиммеричные;

в) симметричные;

г) полусимметричные.

15. Пассивными способами защиты информации являются _____

Ответ: ослабление наводок ПЭМИ в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны.

16. Межсетевой экран служит для _____

Ответ: фильтрации трафика при передачи данных.

17. Хэш-функции предназначены, главным образом, для контроля _____

Ответ: целостности данных.

18. Каким образом в СЗИ Secret Net реализуется настройка дискреционного разграничения доступа к файлам и папкам?

Ответ: настройка дискреционного разграничения доступа к файлам и папкам производится штатными средствами операционной системы.

3.3 Перечень теоретических вопросов к зачету

(для оценки знаний)

1. Основные понятия, термины и определения; предмет и объект защиты;
2. Уязвимости и угрозы безопасности информации в АИС; риски информационной безопасности (ИБ) и методы их оценки;
3. Правовые и организационные методы защиты информации в АИС; аудит ИБ;
4. Базовые принципы организации ЗИ;
5. Защита информации в АИС от несанкционированного доступа (НСД): подсистема идентификации и аутентификации (методы и средства);
6. Модели разграничения доступа к объектам: избирательное управление; мандатное управление; замкнутая программная среда;
7. Архитектура системы защиты информации (СЗИ) от НСД SecretNet;
8. СЗИ от НСД SecretNet: дискреционное разграничение доступа, полномочное разграничение доступа;
9. СЗИ от НСД Dallas Lock: основные функциональные возможности;
10. Электронный замок Соболь-PCI: настройка и эксплуатация; управление пользователями; диагностика устройства; настройка контроля целостности; регистрация событий;
11. Классификация методов криптографического преобразования информации; методы стеганографии и кодирования;

12. Требования к симметричным и асимметричным криптосистемам;
13. Алгоритм DES; свойства стандарта AES;
14. Стандарт ГОСТ 28145-89;
15. Функции хэширования, алгоритм MD5;
16. Электронная подпись; инфраструктура открытых ключей.

3.4 Перечень теоретических вопросов к экзамену

(для оценки знаний)

17. Основные понятия, термины и определения; предмет и объект защиты;
18. Уязвимости и угрозы безопасности информации в АИС; риски информационной безопасности (ИБ) и методы их оценки;
19. Правовые и организационные методы защиты информации в АИС; аудит ИБ;
20. Базовые принципы организации ЗИ;
21. Защита информации в АИС от несанкционированного доступа (НСД): подсистема идентификации и аутентификации (методы и средства);
22. Модели разграничения доступа к объектам: избирательное управление; мандатное управление; замкнутая программная среда;
23. Архитектура системы защиты информации (СЗИ) от НСД SecretNet;
24. СЗИ от НСД SecretNet: дискреционное разграничение доступа, полномочное разграничение доступа;
25. СЗИ от НСД Dallas Lock: основные функциональные возможности;
26. Электронный замок Соболь-PCI: настройка и эксплуатация; управление пользователями; диагностика устройства; настройка контроля целостности; регистрация событий;
27. Классификация методов криптографического преобразования информации; методы стеганографии и кодирования;
28. Требования к симметричным и асимметричным криптосистемам;
29. Алгоритм DES; свойства стандарта AES;
30. Стандарт ГОСТ 28145-89;
31. Функции хэширования, алгоритм MD5;
32. Электронная подпись; инфраструктура открытых ключей.

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

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.

Описание процедур проведения промежуточной аттестации в форме экзамена

и оценивания результатов обучения

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам или в форме компьютерного тестирования.

При проведении промежуточной аттестации в форме собеседования билеты составляются таким образом, чтобы каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; два практических задания: одно из них для оценки умений (выбирается из перечня типовых простых практических заданий к экзамену); другое практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике фондов оценочных средств.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления

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.

Образец экзаменационного билета

<table>
<tr>
<td>ИРГУПС
20__-20__
учебный год</td>
<td>Экзаменационный билет № 1
по дисциплине «<u>Управление информационной безопасностью автоматизированных систем</u>»</td>
<td>Утверждаю:
Заведующий кафедрой
«_____» ИрГУПС
_____</td>
</tr>
<tr>
<td colspan="3">1. Требования к симметричным и асимметричным криптосистемам
2. Базовые принципы организации ЗИ
3. Алгоритм DES; свойства стандарта AES
4. СЗИ от НСД SecretNet: дискреционное разграничение доступа, полномочное разграничение доступа</td>
</tr>
</table>