

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.38 Организационное и правовое обеспечение
информационной безопасности**

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. – 5
Часов по учебному плану (УП) – 180

Формы промежуточной аттестации
очная форма обучения:
экзамен 7 семестр

Очная форма обучения

Распределение часов дисциплины по семестрам

Семестр	7	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
Экзамен	36	36
Итого	180	180

ИРКУТСК

Электронный документ выгружен из ЕИС ФГБОУ ВО ИРГУПС и соответствует оригиналу

Подписант ФГБОУ ВО ИРГУПС Трофимов Ю.А.

00920FD815CE68F8C4CA795540563D259C с 07.02.2024 05:46 по 02.05.2025 05:46 GMT+03:00

Подпись соответствует файлу документа



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, 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	изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем организационно - правового обеспечения информационной безопасности и защиты информации
1.2 Задачи дисциплины	
1	раскрытие места информационной безопасности и защиты информации в системе информационных отношений
2	раскрытие направлений и областей деятельности субъектов информационных отношений, составной частью которых является обеспечение информационной безопасности и защита информации
3	раскрытие взаимосвязи между информационной безопасностью и удовлетворением информационных потребностей субъектов информационных отношений
4	раскрытие значения обеспечения информационной безопасности для предотвращения негативного информационного воздействия на субъекты информационных отношений
5	определение места защиты информации в обеспечении сохранности документальной базы, раскрывающей различные стороны социально-экономического и культурного развития страны
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.15 Управление персоналом
2	Б1.О.18 Правоведение
3	Б1.О.20 Психология в профессиональной деятельности
4	Б1.О.33 Основы информационной безопасности
5	Б1.О.34 Документоведение
6	Б2.О.01(У) Учебная - учебно-лабораторный практикум
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.41 Управление информационной безопасностью
2	Б1.О.50 Комплексная защита в информационных системах персональных данных
3	Б1.О.57 Методы принятия организационно-технических решений
4	Б1.О.61 Технические средства охраны
5	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
6	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические	ОПК-5.1 Знает нормативно-правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Знать: нормативно-правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
		Уметь: применять нормативно-правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

документы, регламентирующие деятельность по защите информации	ОПК-5.2 Способен использовать общеправовые знания для организационных мероприятий по защите информации	Владеть: навыками по применению нормативно-правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации
		Знать: методологию общеправовых знаний для организационных мероприятий по защите информации
		Уметь: применять общеправовые знания для организационных мероприятий по защите информации
		Владеть: навыками по применению общеправовых знаний для организационных мероприятий по защите информации
	ОПК-5.3 Имеет навыки оформления документов по организации защиты информации	Знать: методологию оформления документов по организации защиты информации
		Уметь: применять навыки оформления документов по организации защиты информации
		Владеть: навыками оформления документов по организации защиты информации
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.3 Знает принципы и методы командообразования	Знать: принципы и методы командообразования
		Уметь: применять принципы и методы командообразования
		Владеть: принципами и методами командообразования

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Семестр	Очная форма				*Код индикатора достижения компетенции
			Часы				
			Лек	Пр	Лаб	СР	
1.0	Раздел 1. Правовое обеспечение информационной безопасности.						
1.1	Тема 1. Правовое обеспечение информационной безопасности и пути его совершенствования	7	2			2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.2	Тема 2. Задачи и функции правовой защиты информации	7	2	4		2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.3	Тема 3. Институт правовой защиты государственной тайны	7	2			2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.4	Тема 4. Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ)	7		6		2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.5	Тема 5. Институт правовой защиты коммерческой тайны	7	2			2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.6	Тема 6. Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны	7	1	4		2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.7	Тема 7. Институт правовой защиты профессиональной тайны	7	2			4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.8	Тема 8. Банковская информация и обеспечение банковской тайны	7	2	4		2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.9	Тема 9. Институт правовой защиты информации персонального характера (персональные данные)	7	2			2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.10	Тема 10. Международные и российские документы, касающиеся использования персональных данных и их правовой защиты	7	1	4		2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.11	Тема 11. Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием объектов интеллектуальной	7	2			2	ОПК-5.1 ОПК-5.2 ОПК-5.3

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма				*Код индикатора достижения компетенции
		Семестр	Часы			
			Лек	Пр	Лаб	
	собственности					
1.12	Тема 12. Авторский договор	7	2	6		ОПК-5.1 ОПК-5.2 ОПК-5.3
2.0	Раздел 2. Организационное обеспечение информационной безопасности.					
2.1	Тема 13. Сущность организационного обеспечения информационной безопасности и его место в комплексном обеспечении информационной безопасности и системы защиты информации	7	2			ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3
2.2	Тема 14. Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации	7	2	4		ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3
2.3	Тема 15. Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну	7	2	4		ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3
2.4	Тема 16. Оформление допуска сотрудников к конфиденциальной информации	7	1	4		ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3
2.5	Тема 17. Организация разрешительной системы доступа к конфиденциальной информации	7	2	3		ОПК-5.1 ОПК-5.2 ОПК-5.3
2.6	Тема 18. Организация физической охраны предприятия	7	2	2		ОПК-5.2 ОПК-5.3 УК-3.3
2.7	Тема 19. Организация пропускного и внутри объектового режимов	7	1	2		ОПК-5.2 ОПК-5.3 УК-3.3
2.8	Тема 20. Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями	7	1	2		ОПК-5.2 ОПК-5.3
2.9	Тема 21. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам	7	1	2		ОПК-5.2 ОПК-5.3
	Форма промежуточной аттестации – экзамен	7	36			ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3
	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	Краковский, Ю. М. Информационная безопасность и защита информации :	95

	учеб. пособие / Ю. М. Краковский ; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ. — Иркутск : ИрГУПС, 2016. — 224 с. — Текст : непосредственный.	
6.1.1.2	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
6.1.1.3	Лапина, М. А. Информационное право : учебное пособие / М. А. Лапина, А. Г. Ревин, В. И. Лапин ; под ред. И. Ш. Киясханов. — Москва : Юнити-Дана Закон и право, 2017. — 336 с. — URL: https://biblioclub.ru/index.php?page=book&id=685428 (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	Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. — Москва, Берлин : Директ-Медиа, 2015. — 255 с. — URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 18.04.2024). — 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.О.38 Организационное и правовое обеспечение информационной безопасности по специальности – 10.05.03 Информационная безопасность автоматизированных систем, специализация Безопасность открытых информационных систем / Н.И. Глухов ; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 13 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47630_1529_2024_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	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	MathCAD_student 15.0 Academic_License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01	
6.3.2.2	Python 3.9, свободно распространяемое программное обеспечение https://docs.python.org/3/license.html	
6.3.2.3	Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/	
6.3.2.4	MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01.	
6.3.2.5	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01.	
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	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).
4	Лаборатория Д-523 «Моделирование и разработка программных систем и защита информации». «Безопасность программно-аппаратных средств защиты информации» 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 (переносной), экран (переносной), компьютер
5	Лаборатория Д-525 «Специальные средства и методы защиты информации». «Техническая защита информации» 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 (переносной), экран (переносной), компьютер
6	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	<p>Лекция (от латинского «lectio» – 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.</p> <p>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 пометить 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 удастся разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии</p>
Практическое занятие	<p>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</p>

	<p>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.</p> <p>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</p>
Самостоятельная работа	<p>Обучение по дисциплине «Организационное и правовое обеспечение информационной безопасности» 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 удастся, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора.</p> <p>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»</p>
<p>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</p>	

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 «Организационное и правовое обеспечение информационной безопасности» участвует в формировании компетенций:

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
7 семестр				
1.0	Раздел 1. Правовое обеспечение информационной безопасности			
1.1	Текущий контроль	Тема 1. Правовое обеспечение информационной безопасности и пути его совершенствования	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.2	Текущий контроль	Тема 2. Задачи и функции правовой защиты информации	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.3	Текущий контроль	Тема 3. Институт правовой защиты государственной тайны	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.4	Текущий контроль	Тема 4. Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ)	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.5	Текущий контроль	Тема 5. Институт правовой защиты коммерческой тайны	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.6	Текущий контроль	Тема 6. Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.7	Текущий контроль	Тема 7. Институт правовой защиты профессиональной тайны	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.8	Текущий контроль	Тема 8. Банковская информация и обеспечение банковской тайны	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.9	Текущий контроль	Тема 9. Институт правовой защиты информации персонального характера (персональные данные)	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.10	Текущий контроль	Тема 10. Международные и российские документы, касающиеся использования персональных данных и их правовой защиты	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.11	Текущий контроль	Тема 11. Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием объектов интеллектуальной собственности	ОПК-5.1 ОПК-5.2 ОПК-5.3	Тестирование (компьютерные технологии)
1.12	Текущий контроль	Тема 12. Авторский договор	ОПК-5.1 ОПК-5.2	Собеседование (устно)

			ОПК-5.3	
2.0	Раздел 2. Организационное обеспечение информационной безопасности			
2.1	Текущий контроль	Тема 13. Сущность организационного обеспечения информационной безопасности и его место в комплексном обеспечении информационной безопасности и системы защиты информации	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3	Собеседование (устно)
2.2	Текущий контроль	Тема 14. Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3	Собеседование (устно)
2.3	Текущий контроль	Тема 15. Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3	Собеседование (устно)
2.4	Текущий контроль	Тема 16. Оформление допуска сотрудников к конфиденциальной информации	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3	Тестирование (компьютерные технологии)
2.5	Текущий контроль	Тема 17. Организация разрешительной системы доступа к конфиденциальной информации	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
2.6	Текущий контроль	Тема 18. Организация физической охраны предприятия	ОПК-5.2 ОПК-5.3 УК-3.3	Собеседование (устно)
2.7	Текущий контроль	Тема 19. Организация пропускного и внутри объектового режимов	ОПК-5.2 ОПК-5.3 УК-3.3	Собеседование (устно)
2.8	Текущий контроль	Тема 20. Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями	ОПК-5.2 ОПК-5.3	Собеседование (устно)
2.9	Текущий контроль	Тема 21. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам	ОПК-5.2 ОПК-5.3	Собеседование (устно)
	Промежуточная аттестация	Все разделы	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3	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
2	Тестирование (компьютерные технологии)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	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
2	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 экзамена. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	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 неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	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 экзамена

Критерии оценивания	Шкала оценивания
Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования	«отлично»
Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования	«хорошо»
Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования	«удовлетворительно»
Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования	«неудовлетворительно»

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»

Тестирование

Шкалы 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

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

1. Резервирование и восстановление информации; повышение надежности АИС;
2. Блокировка ошибочных операций пользователей; минимизация ущерба от аварий и стихийных бедствий;
3. Инженерно-физическая защита объектов информатизации; система контроля и управления доступом;
4. Организация работ с конфиденциальными информационными ресурсами;
5. защита от злоумышленных действий обслуживающего персонала и пользователей;
6. Понятие и возможности DLP-систем;
7. Методы и средства защиты информации в АИС от утечек по техническим каналам;
8. Противодействие наблюдению в оптическом диапазоне; противодействие утечкам по группе акустических каналов;
9. Методы и средства защиты от побочных электромагнитных излучений и наводок;
10. Компьютерные вирусы; троянские программы; сетевые черви; сертифицированные средства антивирусной защиты;
11. Средства сетевой безопасности: межсетевые экраны, сканеры безопасности;
12. Средства сетевой безопасности: средства построения виртуальных частных сетей (VPN), системы обнаружения вторжений.

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-5.1 ОПК-5.2 ОПК-5.3	Тема 1. Правовое обеспечение информационной безопасности и пути его совершенствования	Знание	1 – ОТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 2. Задачи и функции правовой защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 3. Институт правовой защиты государственной тайны	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ

		Навык	1 – ОТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 4. Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ)	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 5. Институт правовой защиты коммерческой тайны	Знание	1 – ОТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 6. Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 7. Институт правовой защиты профессиональной тайны	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 8. Банковская информация и обеспечение банковской тайны	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 9. Институт правовой защиты информации персонального характера (персональные данные)	Знание	1 – ОТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 10. Международные и российские документы, касающиеся использования персональных данных и их правовой защиты	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 11. Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием объектов интеллектуальной собственности	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 12. Авторский договор	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3	Тема 13. Сущность организационного обеспечения информационной безопасности и его место в комплексном обеспечении информационной безопасности и системы защиты информации	Знание	1 – ОТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3	Тема 14. Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3	Тема 15. Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3 УК-3.3	Тема 16. Оформление допуска сотрудников к конфиденциальной информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.1 ОПК-5.2	Тема 17. Организация разрешительной системы доступа к конфиденциальной информации	Знание	1 – ОТЗ 1 – ЗТЗ

ОПК-5.3		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-5.2 ОПК-5.3 УК-3.3	Тема 18. Организация физической охраны предприятия	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.2 ОПК-5.3 УК-3.3	Тема 19. Организация пропускного и внутри объектового режимов	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-5.2 ОПК-5.3	Тема 20. Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ОПК-5.2 ОПК-5.3	Тема 21. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам	Знание	1 – ОТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	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. Выберите правильное определение термина «информация»:
 - а) совокупность содержащихся в базах данных сведений;
 - б) совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях;
 - в) сведения (сообщения, данные) воспроизводимые различными системами;
 - г) **сведения (сообщения, данные) независимо от формы их представления.**

2. Выберите правильное определение термина «обладатель информации»:
 - а) лицо, самостоятельно создавшее информацию;
 - б) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;
 - в) **лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;**
 - г) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

3. Предоставление информации – это

Ответ: действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

4. Защищаемые помещения – это

Ответ: помещения, специально предназначенные для проведения конфиденциальных мероприятий.

5. Выберите правильное определение термина «контролируемая зона»:

- а) пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;**
- б) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств;
- в) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации;
- г) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей.

6. 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.**

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. Максимально возможное количество категорий конфиденциальности в СЗИ Secret Net 7.x равно ____

Ответ: 16.

10. 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.

11. Несанкционированный доступ к информации – это

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

12. Механизм контроля целостности СЗИ Secret Net предназначен для

- а) формирования цифровых отпечатков данных;
- б) контроля информационных потоков;

в) слежения за неизменностью содержимого ресурсов компьютера.

13. 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.

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

- а) «конфиденциально»;**
- б) «секретно»;
- в) «строго конфиденциально»,
- г) «неконфиденциально».**

15. Практическая стойкость алгоритма Диффи-Хеллмана основана на сложности решения задачи нахождения дискретного _____

Ответ: логарифма.

16. Хэш-функции предназначены, главным образом, для _____

Ответ: контроля целостности данных.

17. Длина хэш-кода алгоритма MD5 составляет _____

Ответ: 128 бит.

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 экзамену

(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.

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
Тестирование (компьютерные технологии)	Тестирование проводится по результатам освоения тем или разделов дисциплины или по окончании ее изучения во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте, время выполнения. Результаты тестирования видны обучающемуся на компьютере сразу после прохождения теста

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 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

 <p>ИрГУПС 20__-20__ учебный год</p>	<p>Экзаменационный билет № 1 по дисциплине «<u>Организационное и правовое обеспечение информационной безопасности</u>»</p>	<p>Утверждаю: Заведующий кафедрой « _____ » ИрГУПС _____</p>
<ol style="list-style-type: none">1. Требования к симметричным и асимметричным криптосистемам2. Базовые принципы организации ЗИ3. Алгоритм DES; свойства стандарта AES4. СЗИ от НСД SecretNet: дискреционное разграничение доступа, полномочное разграничение доступа		