ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом и.о. ректора
от «07» июня 2021 г. № 79

Б1.О.27 Основы информационной безопасности

рабочая программа дисциплины

Специальность/направление подготовки – 10.03.01 Информационная безопасность
Специализация/профиль – Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника – Бакалавр
Форма и срок обучения – очная форма 4 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:
экзамен 2 семестр, курсовая работа 2 семестр

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

Семестр	2	**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 – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427.

Программу составил(и):
к.э.н., доцент, С.П.Серёдкин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «4» июня 2021 г. № 11-2

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

1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цель дисциплины	
1	раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристика составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов
1.2 Задачи дисциплины	
1	изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации
2	изучение видов защищаемой информации, угроз информационной безопасности, методов и средств обеспечения информационной безопасности, механизмов защиты информации, моделей безопасности, критериев оценки защищенности и обеспечения безопасности информационных систем
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового – 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 воспитания 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.47 Теоретические основы компьютерной безопасности
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.31 Организационное и правовое обеспечение информационной безопасности
2	Б1.О.36 Основы управления информационной безопасностью
3	Б1.О.51 Безопасность систем баз данных
4	Б1.О.52 Аудит информационной безопасности
5	Б1.О.53 Методология построения защищенных автоматизированных систем
6	Б2.О.01(У) Учебная - ознакомительная практика
7	Б2.О.02(У) Учебная - учебно-лабораторная практика
8	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
9	Б3.02(Д) Защита выпускной квалификационной работы

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для	ОПК-1.1 Знает сущность и значение информации, информационных технологий и информационной безопасности в развитии современного общества	Знать: сущность и значение информации, информационных технологий и информационной безопасности в развитии современного общества
		Уметь: реализовывать на практике знания о сущности и значении информации, информационных технологий и информационной безопасности в развитии современного общества
		Владеть: навыками работ по реализации знаний по сущности и значению информации, информационных технологий и информационной безопасности в развитии

обеспечения объективных потребностей личности, общества и государства;		современного общества
	ОПК-1.2 Умеет пользоваться нормативными документами, современным программным обеспечением в области информационной безопасности	Знать: нормативные документы с современным программным обеспечением в области информационной безопасности
		Уметь: пользоваться нормативными документами с современным программным обеспечением в области информационной безопасности
		Владеть: навыками работ по реализации знаний нормативных документов с современным программным обеспечением в области информационной безопасности
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1 Знает основные принципы административно-правовой защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знать: основные принципы административно-правовой защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
		Уметь: применять основные принципы административно-правовой защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
		Владеть: навыками применения основных принципов административно-правовой защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
	ОПК-6.2 Умеет быстро реагировать на различные угрозы информационной безопасности и организовывает защиту информации ограниченного доступа	Знать: различные угрозы информационной безопасности и способы организации защиты организовывать информации ограниченного доступа
		Уметь: быстро реагировать на различные угрозы информационной безопасности и организовывать защиту информации ограниченного доступа
		Владеть: навыками реагирования на различные угрозы информационной безопасности и организовывать защиту информации ограниченного доступа
	ОПК-6.3 Имеет навыки организации защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знать: нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
		Уметь: применять навыки организации защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
		Владеть: навыками реагирования на различные угрозы информационной безопасности и организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

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 Теория информационной безопасности.**						

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.1	Сущность и понятие информационной безопасности	2	8	11		11	ОПК-1.2 ОПК-6.1
2.0	**Раздел 2 Методология защиты информации.**						
2.1	Сущность и понятие защиты информации	2	6	10		12	ОПК-1.1 ОПК-1.2 ОПК-6.1 ОПК-6.3
2.2	Теоретические и концептуальные основы защиты информации	2	8	10		12	ОПК-1.2 ОПК-6.2 ОПК-6.3
2.3	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности	2	6	10		12	ОПК-6.1 ОПК-6.2 ОПК-6.3
2.4	Классификация видов, методов и средств защиты информации	2	6	10		12	ОПК-1.2 ОПК-6.1 ОПК-6.2
	Форма промежуточной аттестации – экзамен	2	36				ОПК-1.1 ОПК-1.2 ОПК-6.1 ОПК-6.2 ОПК-6.3
	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	Документальное обеспечение информационной безопасности : учебное пособие для студентов, обучающихся по направлению 10.03.01 «информационная безопасность». — Севастополь : СевГУ, 2022. — 142 с. — URL: https://e.lanbook.com/book/261899 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Ванюшина, А. В. Основы информационной безопасности : учебно-методическое пособие для студентов цзопб. направление подготовки: 09.03.02 / А. В. Ванюшина, С. Ю. Рыбаков. — Москва : МТУСИ, 2022. — 22 с. — URL: https://e.lanbook.com/book/333701 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.3	Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Юрайт, 2021. — 104 с. — URL: https://urait.ru/bcode/477968 (дата обращения: 22.04.2024). — Текст : электронный.	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Глухов, Н. И. Информационная безопасность предпринимательской деятельности : учеб. пособие / Н. И. Глухов ; Сибир. ин-т права, экономики и	3

	упр. — Иркутск : СПЭУ, 2008. — 327 с. — Текст : непосредственный.	
6.1.2.2	Информационные технологии : лабораторный практикум. специальности: 10.05.03 – информационная безопасность автоматизированных систем; 11.03.02 –инфокоммуникационные технологии и системы связи. — Ставрополь : СКФУ, 2016. — 168 с. — URL: https://e.lanbook.com/book/155224 (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	Серёдкин, С.П. Методические указания по изучению дисциплины Б1.О.27 Основы информационной безопасности по направлению подготовки 10.03.01 Информационная безопасность, профиль Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности) / С.П. Серёдкин; ИрГУПС. – Иркутск: ИрГУПС, 2021. – 14 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_4252_1480_2021_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 «Образовательная платформа ЮРАЙТ», https://urait.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-415 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-408 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, компьютер
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных

	процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Основы 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 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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости

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

Б1.О.27 Основы информационной безопасности участвует в формировании компетенций:

ОПК-7 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
2 семестр				
1.0	**Раздел 1. Теория информационной безопасности**			
1.1	Текущий контроль	Сущность и понятие информационной безопасности	ОПК-7	Конспект (письменно) Реферирование текста (устно/письменно)
1.2	Текущий контроль	Современная Доктрина информационной безопасности Российской Федерации	ОПК-7	Конспект (письменно) Реферирование текста (устно/письменно)
2.0	**Раздел 2. Методология защиты информации**			
2.1	Текущий контроль	Сущность и понятие защиты информации	ОПК-7	Конспект (письменно)
2.2	Текущий контроль	Теоретические и концептуальные основы защиты информации	ОПК-7	Конспект (письменно) Собеседование (устно)
2.3	Текущий контроль	Организационные основы и методологические принципы защиты информации	ОПК-7	Конспект (письменно)
2.4	Текущий контроль	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности	ОПК-7	Конспект (письменно) Реферирование текста (устно/письменно)
2.5	Текущий контроль	Каналы и методы несанкционированного доступа к конфиденциальной информации	ОПК-7	Конспект (письменно) Реферирование текста (устно/письменно)
2.6	Текущий контроль	Классификация видов, методов и средств защиты информации	ОПК-7	Конспект (письменно) Реферирование текста (устно/письменно)
	Промежуточная аттестация	Раздел 1. Теория информационной безопасности Раздел 2. Методология защиты информации	ОПК-7	Зачет (собеседование) Зачет - тестирование (компьютерные технологии)

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

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

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

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

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

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

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
2	Доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов
3	Конспект	Особый вид текста, в основе которого лежит аналитико-синтетическая переработка информации первоисточника (исходного текста). Цель этой деятельности — выявление, систематизация и обобщение (с возможной критической оценкой) наиболее ценной (для конспектирующего) информации. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы конспектов
4	Реферирование текста	Средство, позволяющее оценивать и диагностировать умения анализировать, синтезировать, обобщать прочитанное с формулированием конкретных выводов, установлением причинно-следственных связей. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Тексты для реферирования (статьи средств массовой информации, научные статьи, профессионально-ориентированные тексты), план (шаблон) реферирования

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	Перечень теоретических

		дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	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

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.

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета

Шкалы оценивания	Критерии оценивания
«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
	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
	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
«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

Критерии и шкала оценивания промежуточной аттестации
в форме компьютерного тестирования

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

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

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

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

Доклад

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

Конспект

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Конспект по теме выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся по заданной теме в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; раскрыл тему полностью и ответил на все вопросы преподавателя по конкретной теме конспекта. Конспект оформлен аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»		Конспект по теме выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся по заданной теме в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; раскрыл тему не полностью и ответил на часть вопросов преподавателя по конкретной теме конспекта. Конспект оформлен аккуратно, с незначительными исправлениями
«удовлетворительно»		Конспект по теме выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся по заданной теме в не полном объеме с частичным соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; раскрыл тему не полностью и ответил на часть вопросов преподавателя по конкретной теме конспекта. Конспект оформлен не аккуратно
«неудовлетворительно»	«не зачтено»	Конспект по теме не выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся не по заданной теме в не полном объеме без соблюдения необходимой последовательности. Обучающийся работал не самостоятельно; не раскрыл тему и не ответил на вопросы преподавателя по конкретной теме конспекта. Конспект оформлен не аккуратно

Реферирование текста

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Текст построен в соответствии с планом (шаблоном) реферирования, логически правильно, имеется введение, основная часть и заключение. Допущено не более 2 лексических, стилистических или грамматических ошибок. Реферирование текста осуществлено в полном объеме; имеется логическая и языковая связность на протяжении всего текста
«хорошо»		Текст построен в соответствии с плану (шаблону) реферирования, логически правильно, имеется введение, основная часть и заключение. Допущено не более 4 лексических, стилистических или грамматических ошибок. Реферирование текста осуществлено в достаточном объеме; имеется логическая и языковая связность на протяжении всего текста.
«удовлетворительно»		Текст не в полной мере соответствует плану (шаблону) реферирования или выстроен логически неправильно, отсутствуют некоторые требуемые структурные части. Допущено не более 7 лексических, стилистических или грамматических ошибок, приведших к недопониманию или непониманию. Реферирование текста осуществлено в недостаточном объеме; имеются неточности в логической и языковой связности текста
«неудовлетворительно»	«не зачтено»	Текст не соответствует планом (шаблоном) реферирования, выстроен логически неправильно. Допущено более 7 языковых ошибок, приведших к недопониманию или непониманию. Реферирование текста осуществлено в недостаточном объеме; имеются неточности в логической и языковой связности на протяжении всего текста

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 перечень вопросов для проведения собеседований.

1. Виды и состав угроз информационной безопасности.
2. Задачи, принципы и методы обеспечения информационной безопасности.
3. Критерии, условия, принципы и формы отнесения информации к защищаемой.
4. Анализ существующих подходов к классификации конфиденциальной информации по видам тайны.
5. Виды и характеристика носителей защищаемой информации.
6. Структура и характеристика угроз защищаемой информации.
7. Соотношение угроз защищаемой информации с видами носителей и формами проявления уязвимости информации.
8. Соотношение видов разведывательной деятельности с каналами и методами несанкционированного доступа к конфиденциальной информации.
9. Классификация и характеристика объектов защиты информации.
10. Классификация и характеристика видов, методов и средств защиты информации и их соотношение с объектами защиты.
11. Сущность, назначение и структура систем защиты информации.
12. Состав угроз информационной безопасности.
13. Методы обеспечения информационной безопасности.
14. Значение защиты информации во внешнеполитической деятельности.
15. Значение защиты информации в военной области.
16. Значение защиты информации в экономической сфере.
17. Социальные последствия защиты информации.
18. Влияние политико-правовых и социально-экономических реальностей на защиту информации.
19. Основные положения теории защиты информации.
20. Понятие и назначение концепции защиты информации.
21. Социально-экономические и организационно-правовые аспекты концепции защиты информации.
22. Требования к концепции защиты информации.
23. Уровни концепции защиты информации.
24. Понятие «носитель защищаемой информации». Способы фиксирования информации в носителях.
25. Свойства и значение типов носителей защищаемой информации. Соотношение видов носителей информации с категориями защищаемой информации и формами проявления ее уязвимости.
26. Показатели разделения конфиденциальной информации на виды тайны.
27. Общее и различия между степенью и грифом конфиденциальности (секретности).
28. Сферы действия государственной и служебной тайны.
29. Сферы действия коммерческой тайны.
30. Сферы действия личной и профессиональной тайны.
31. Формы собственности на информацию.
32. Собственники и владельцы информации, составляющей различные виды тайны.
33. Современные подходы к понятию угрозы защищаемой информации.
34. Признаки и составляющие угрозы защищаемой информации.
35. Состав и характеристика источников дестабилизирующего воздействия на информацию.

36. Виды и способы дестабилизирующего воздействия на информацию со стороны людей.

37. Виды и способы дестабилизирующего воздействия на информацию средств обработки, передачи информации и систем обеспечения их функционирования.

38. Соотношение видов дестабилизирующего воздействия на информацию с формами проявления уязвимости информации.

39. Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на информацию.

40. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию со стороны людей.

41. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию средств обработки, передачи информации и систем обеспечения их функционирования.

42. Соотношение каналов несанкционированного доступа к информации с каналами утечки информации.

43. Соотношение каналов несанкционированного доступа к информации с источниками дестабилизирующего воздействия на информацию.

44. Методы несанкционированного доступа к информации через допущенных к ней лиц.

45. Методы несанкционированного доступа к информации через агентуру.

46. Методы несанкционированного доступа к информации через средства обработки, передачи информации и системы обеспечения их функционирования.

47. Методы несанкционированного физического проникновения на защищаемый объект.

48. Соотношение методов несанкционированного доступа к информации с используемыми техническими средствами.

49. Органы политической, военной и радиотехнической разведки в США.

50. Органы политической и военной разведки ведущих стран Западной Европы.

51. Соотношение между видами и направлениями разведывательной деятельности.

52. Состав подлежащих защите объектов хранения информации.

53. Состав подлежащих защите технических средств изготовления, обработки, воспроизведения и передачи информации.

54. Виды и способы дестабилизирующего воздействия на объекты защиты информации.

55. Классификация видов защиты информации.

56. Классификация методов защиты информации.

57. Классификация программных и криптографических средств защиты информации.

58. Классификация технических средств защиты информации.

59. Полномочия руководства предприятия и служб защиты информации в области защиты информации.

60. Состав и значение ресурсного обеспечения защиты информации.

61. Состав и сферы действия систем защиты информации.

62. Сущность и значение комплексной системы защиты информации.

3.2 Типовые контрольные темы для написания докладов

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

Ниже приведен образец типовых вариантов тем для написания докладов.

1. Структура государственной системы защиты информации (схема).

2. Система документации по технической защите информации (схема).

3. Действующие документы по защите информации с учетом категорий доступа к ней и видов информационных систем.

4. Определение информационной безопасности.

5. Определение защиты информации.
6. Меры по обеспечению информационной безопасности.
7. Основные организационно-технические мероприятиям по защите информации.
8. Источники угрозы информационной безопасности.
9. Угрозы информационной безопасности.
10. Уязвимости информационной безопасности.
11. Атаки информационной безопасности.
12. Построить логическую цепочку реализации угрозы информационной безопасности.
13. Построить схему классификации источников угроз ИБ.
14. Объективные уязвимости.
15. Субъективные уязвимости.
16. Случайные уязвимости.
17. Понятие лицензии (пользовательская лицензия).
18. Определение лицензионной политики.
19. Понятие коммерческой лицензии.
20. Понятие открытой лицензии.
21. Гарантируемые права открытой лицензии.
22. Понятие нелицензионного программного обеспечения.
23. Угрозы при использовании нелицензионного программного обеспечения.
24. Закон, определяющий правовые основы информационной безопасности (наименование, когда принят, основные требования).

3.3 Типовые контрольные задания для написания конспекта

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

Ниже приведен образец типовых вариантов заданий для написания конспектов.

1. Виды и состав угроз информационной безопасности.
2. Задачи, принципы и методы обеспечения информационной безопасности.
3. Критерии, условия, принципы и формы отнесения информации к защищаемой.
4. Анализ существующих подходов к классификации конфиденциальной информации по видам тайны.
5. Виды и характеристика носителей защищаемой информации.
6. Структура и характеристика угроз защищаемой информации.
7. Соотношение угроз защищаемой информации с видами носителей и формами проявления уязвимости информации.
8. Соотношение видов разведывательной деятельности с каналами и методами несанкционированного доступа к конфиденциальной информации.
9. Классификация и характеристика объектов защиты информации.
10. Классификация и характеристика видов, методов и средств защиты информации и их соотношение с объектами защиты.
11. Сущность, назначение и структура систем защиты информации.
12. Состав угроз информационной безопасности.
13. Методы обеспечения информационной безопасности.
14. Значение защиты информации во внешнеполитической деятельности.
15. Значение защиты информации в военной области.
16. Значение защиты информации в экономической сфере.
17. Социальные последствия защиты информации.
18. Влияние политико-правовых и социально-экономических реальностей на защиту информации.
19. Основные положения теории защиты информации.
20. Понятие и назначение концепции защиты информации.
21. Социально-экономические и организационно-правовые аспекты концепции защиты информации.

22. Требования к концепции защиты информации.
23. Уровни концепции защиты информации.
24. Понятие «носитель защищаемой информации». Способы фиксирования информации в носителях.
25. Свойства и значение типов носителей защищаемой информации. Соотношение видов носителей информации с категориями защищаемой информации и формами проявления ее уязвимости.
26. Показатели разделения конфиденциальной информации на виды тайны.
27. Общее и различия между степенью и грифом конфиденциальности (секретности).
28. Сферы действия государственной и служебной тайны.
29. Сферы действия коммерческой тайны.
30. Сферы действия личной и профессиональной тайны.
31. Формы собственности на информацию.
32. Собственники и владельцы информации, составляющей различные виды тайны.
33. Современные подходы к понятию угрозы защищаемой информации.
34. Признаки и составляющие угрозы защищаемой информации.
35. Состав и характеристика источников дестабилизирующего воздействия на информацию.
36. Виды и способы дестабилизирующего воздействия на информацию со стороны людей.
37. Виды и способы дестабилизирующего воздействия на информацию средств обработки, передачи информации и систем обеспечения их функционирования.
38. Соотношение видов дестабилизирующего воздействия на информацию с формами проявления уязвимости информации.
39. Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на информацию.
40. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию со стороны людей.
41. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию средств обработки, передачи информации и систем обеспечения их функционирования.

3.4 Типовые контрольные задания для реферирования текста

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

Ниже приведен образец типовых вариантов заданий для реферирования текста.

1. Соотношение каналов несанкционированного доступа к информации с каналами утечки информации.
2. Соотношение каналов несанкционированного доступа к информации с источниками дестабилизирующего воздействия на информацию.
3. Методы несанкционированного доступа к информации через допущенных к ней лиц.
4. Методы несанкционированного доступа к информации через агентуру.
5. Методы несанкционированного доступа к информации через средства обработки, передачи информации и системы обеспечения их функционирования.
6. Методы несанкционированного физического проникновения на защищаемый объект.
7. Соотношение методов несанкционированного доступа к информации с используемыми техническими средствами.
8. Органы политической, военной и радиотехнической разведки в США.
9. Органы политической и военной разведки ведущих стран Западной Европы.
10. Соотношение между видами и направлениями разведывательной деятельности.
11. Состав подлежащих защите объектов хранения информации.
12. Состав подлежащих защите технических средств изготовления, обработки, воспроизведения и передачи информации.

13. Виды и способы дестабилизирующего воздействия на объекты защиты информации.
14. Классификация видов защиты информации.
15. Классификация методов защиты информации.
16. Классификация программных и криптографических средств защиты информации.
17. Классификация технических средств защиты информации.
18. Полномочия руководства предприятия и служб защиты информации в области защиты информации.
19. Состав и значение ресурсного обеспечения защиты информации.
20. Состав и сферы действия систем защиты информации.
21. Сущность и значение комплексной системы защиты информации.

3.5 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-7.2	Сущность и понятие информационной безопасности	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
ОПК-7.2	Современная Доктрина информационной безопасности Российской Федерации	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 3 – ЗТЗ
ОПК-7.2	Сущность и понятие защиты информации Теоретические и концептуальные основы защиты информации Организационные основы и методологические принципы защиты информации	Знание	4 – ОТЗ 3 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 3 – ЗТЗ
ОПК-7.2	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности Каналы и методы несанкционированного доступа к конфиденциальной информации	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	3 – ОТЗ 3 – ЗТЗ
ОПК-7.2	Сущность и понятие защиты информации Теоретические и концептуальные основы защиты информации Организационные основы и методологические принципы защиты информации	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
ОПК-7.2	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности		
ОПК-7.2	Каналы и методы несанкционированного доступа к конфиденциальной информации Сущность и понятие защиты информации	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ

ОПК-7.2	Теоретические и концептуальные основы защиты информации	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Навык	3 – ОТЗ 3 – 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 теста для проведения промежуточной аттестации в форме зачета за 2 семестр по дисциплине «Основы информационной безопасности»

Описание требований к тесту:

1.Виды и количество предъявляемых обучающемуся тестовых заданий.

Тест состоит из следующих типов тестовых заданий:

ТЗ типа А: тестовое задание закрытой формы (ТЗ с выбором одного или нескольких правильных ответов);

ТЗ типа В: тестовое задание открытой формы (с кратким регламентируемым ответом)

ТЗ типа С: тестовое задание на установление соответствия;

ТЗ типа Д: тестовое задание на установление правильной последовательности.

Количество тестовых заданий по типам:

6 – тип А

6 – тип В

2 – тип С

1 – тип D

2. Критерии оценки:

Результаты тестирования	Оценка
Обучающийся набрал при тестировании более 50 баллов	«зачтено»
Обучающийся набрал при тестировании менее 50 баллов	«не зачтено»

3. Норма времени: на выполнение теста отводится 60 минут.

4. Дополнительные требования: использование литературы, справочников и лекций не допускается.

Образец типового теста содержит задания для оценки знаний, для оценки умений, для оценки навыков и (или) опыта деятельности.

Пример теста для проведения промежуточной аттестации в форме зачета за 2 семестр по дисциплине «Основы информационной безопасности»

1. Определение термина «информация»:

А - совокупность содержащихся в базах данных сведений;

Б - сведения (сообщения, данные) независимо от формы их представления.

В - сведения (сообщения, данные) воспроизводимые различными системами.

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

2. 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.

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

3. Технические способы защиты информации в зависимости от используемых средств классифицируются как:

А - полуактивные;

Б - пассивные;

В – разноплановые.

Ответ: Б – пассивные.

4. Указать меры, которые устанавливаются для обеспечения правового режима защиты персональных данных;

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры.

5. Указать источники права в области оборота сведений составляющих коммерческую тайну;

Федеральный закон от 29.07.2004 N 98-ФЗ О коммерческой тайне.

6. Если сведения относятся к государственной тайне проанализировать порядок установления степени их секретности грифов секретности:

1- «особой важности»;

2- «совершенно секретно»;

3- «секретно».

7. Пассивные способы защиты информации:

А - экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры;

Б - ослабление наводок ПЭМИ в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны;

В - создание маскирующих электромагнитных помех в цепях заземления.

Ответ: А - экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры.

8. Несанкционированный доступ к информации:

А - доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

Б - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;

В - доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация.

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

9. 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.

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

10. Построить схему реализации угрозы информационной безопасности в атаку.

11. Защита информации представляет собой принятие мер, перечислить.

Правовые, организационные и технические меры.

12. Исходя из требований № 149-ФЗ защиту информации можно разделить так же на несколько уровней:

Общедоступную и ограниченного доступа.

13. Свойства безопасности информации, перечислить.

Конфиденциальность, целостность, доступность.

14. Способы и методы защиты электронного документооборота, назвать:

Правовые, организационные, технические меры обеспечивающие;

- **Защиту информации от несанкционированного доступа, уничтожения, модификации, блокирования, копирования, фальсификации, распространения, а также от других несанкционированных действий в отношении такой информации;**
- **Соблюдение конфиденциальности информации ограниченного доступа;**
- **Реализацию права на доступ к информации.**

15. Риск информационной безопасности:

А – потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.

Б – потенциальная возможность нанесения ущерба в результате действия угроз информационной безопасности;

В – возможность реализации угрозы информационной безопасности;

Г – неудовлетворительное состояние системы защиты информации.

Ответ: А – потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.

15. Ответственность за нарушение требований в области обеспечения информационной безопасности:

Ответ: дисциплинарная, гражданско-правовая, административная и уголовная ответственность.

16. Назначение модели угроз безопасности информации:

А- формирование требований к защите информации;

Б- выявление угроз информационной безопасности;

В- определение актуальных угроз безопасности информации.

Ответ: А- формирование требований к защите информации.

17. Угроза информационной безопасности?

Ответ: системы безопасности создаются в отношении всех значимых объектов критической информационной инфраструктуры.

18. Политика информационной безопасности:

А- Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности;

Б- Документ содержащий требования к обеспечению защиты информации;

В- Правила поведения сотрудников организации в вопросах обеспечения информационной безопасности.

Ответ: А- Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

3.6 Перечень теоретических вопросов к зачету

(для оценки знаний)

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Определение информационной безопасности
4. Место информационной безопасности в системе национальной безопасности
5. Интересы личности в информационной сфере
6. Интересы общества в информационной сфере

7. Интересы государства в информационной сфере
8. Угрозы информационному обеспечению государственной политики Российской Федерации
9. Виды угроз информационной безопасности
10. Внешние источники угроз информационной безопасности
11. Внутренние источники угроз информационной безопасности государства.
12. Информационное оружие, его классификация и возможности.
13. Доктрина информационной войны
14. Методы и средства ведения информационной войны
15. Понятие информационного противоборства
16. Причины искажения информации
17. Виды искажения информации
18. Каналы утечки информации
19. Естественные и искусственные каналы утечки информации
20. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств ВТ
22. Компьютерная система как объект информационной безопасности.
23. Информационные процессы как объект информационной безопасности
24. Влияние человеческого фактора на обеспечение информационной безопасности
25. Программно-аппаратные средства обеспечения информационной безопасности.
26. Классификация программно-аппаратных средств обеспечения информационной безопасности
27. Защита от несанкционированного доступа
28. Антивирусная защита
29. Межсетевые экраны
30. VPN-технологии
31. Криптографические методы защиты информации

3.7 Перечень типовых простых практических заданий к зачету

(для оценки умений)

1.Привести практические примеры использования системы обнаружения вторжений и анализа защищённости.
2. Представить схему работы сетевых сканеров.
3. Перечислить критерии анализа защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности.

3.8 Перечень типовых практических заданий к экзамену

(для оценки навыков и (или) опыта деятельности)

1. Понятие национальной безопасности в нормативно-правовых документах РФ.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Определение информационной безопасности
4. Место информационной безопасности в системе национальной безопасности
5. Интересы личности в информационной сфере
6. Интересы общества в информационной сфере
7. Интересы государства в информационной сфере
8. Угрозы информационному обеспечению государственной политики Российской Федерации

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
Доклад	Защита докладов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему докладов и требования, предъявляемые к их выполнению и защите
Конспект	Защита конспектов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему конспектов и требования, предъявляемые к их выполнению и защите
Реферирование текста	Выполнение реферирования текста, предусмотренного рабочей программой дисциплины, выполняется обучающимся во время практического занятия или в часы, выделенные на самостоятельную работу. Во время выполнения задания пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не рекомендуется. Обязательными требованиями являются четкое соблюдения структуры, предложенной в плане (шаблоне) реферирования, использование лексики реферируемого текста, достаточного количества слов-связок. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся требования к выполнению задания и отведенное время на их выполнение время, предоставляет план (шаблон), список рекомендуемых фраз-клише и слов-связок для реферирования текста. Преподаватель информирует о результатах оценивания работы на текущем занятии после выполнения обучающимся задания, в обязательном порядке аргументирует выставленную оценку, дает рекомендации по улучшению структуры и содержания работы

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 процедуры проведения промежуточной аттестации в форме зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель проводит итоговое тестирование по дисциплине. Промежуточная аттестация в форме зачета с проведением аттестационного испытания в форме тестирования проходит на последнем занятии по дисциплине. На выполнение итогового тестирования отводится 60 минут. Использование лекций и различной литературы запрещено.

Перечень вопросов для подготовки к зачету (итоговому тестированию по дисциплине) обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета

Результаты тестирования	Оценка
Обучающийся набрал при тестировании более 50 баллов	«зачтено»

Обучающийся набрал при тестировании менее 50 баллов	«не зачтено»