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 «17» июня 2022 г. № 77

Б1.О.55 Защита объектов критической информационной инфраструктуры

рабочая программа дисциплины

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

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

Формы промежуточной аттестации
очная форма обучения:
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*	68	**68**
– лекции	34	**34**
– практические (семинарские)	34	**34**
– лабораторные		
Самостоятельная работа	40	**40**
Экзамен	36	**36**
Итого	144	**144**

ИРКУТСК

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

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

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «17» июня 2022 г. № 12

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

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели дисциплины

1	формирование у обучающихся системных знаний по обеспечению информационной безопасности критической информационной инфраструктуры;
2	формирование у обучающихся практических навыков по разработке и реализации планов реагирования на компьютерные инциденты

1.2 Задачи дисциплины

1	формирование системных знаний о значимых объектах критической информационной инфраструктуры, а также методах и средствах обеспечения их безопасности;
2	изучение нормативно-правовых актов по безопасности критической информационной инфраструктуры;
3	изучение методов оценки уровня защищенности (аудита) систем и сетей и содержащейся в них информации;
4	освоение необходимых знаний по проведению категорирования объектов критической информационной инфраструктуры;
5	формирование умений и знаний по проведению оценки угроз безопасности информации на объектах критической информационной инфраструктуры;
6	изучение механизма проведения инвентаризации систем и сетей, анализ уязвимостей, тестирование на проникновение систем и сетей с использованием соответствующих автоматизированных средств;
7	освоение методов организации и планирования мероприятий по обеспечению безопасности объектов критической информационной инфраструктуры

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.36 Сети и системы передачи информации
2	Б1.О.37 Защита информации от утечки по техническим каналам
3	Б1.О.47 Информационные технологии
4	Б1.О.51 Кибербезопасность

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

1	Б1.О.39 Программно-аппаратные средства защиты информации
2	Б1.О.41 Управление информационной безопасностью
3	Б1.О.45 Виртуальные частные сети
4	Б1.О.50 Комплексная защита в информационных системах персональных данных
5	Б1.О.62 Моделирование процессов и систем защиты информации
6	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
7	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-5.1 Способен разрабатывать и	ОПК-5.1.1 Знает особенности разработки политики информационной	Знать: нормативно правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов

реализовывать политику информационной безопасности открытых информационных систем	безопасности открытых информационных систем	критической информационной инфраструктуры (КИИ); процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ
		Уметь: выявлять и анализировать угрозы безопасности информации по результатам возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации
		Владеть: навыками работы с нормативно правовыми актами, методическими документами и национальными стандартами в области обеспечения безопасности значимых объектов КИИ
	ОПК-5.1.2 Умеет формировать исходные требования для разработки политики информационной безопасности	Знать: требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ; требования к программным и программно-аппаратным средствам, принимаемым для обеспечения безопасности значимых объектов КИИ
		Уметь: обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ; формировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий
		Владеть: навыками работы с базами данных, содержащую информацию по угрозам безопасности информации м уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами; навыками разработки организационно-распорядительных документов по безопасности значимых объектов КИИ; навыками участия в разработке организационных и технических мероприятий по защите объектов КИИ
	ОПК-5.1.3 Имеет навыки обоснования целесообразности реализации политики информационной безопасности открытых информационных систем	Знать: процедуру подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий; порядок обработки результатов контроля (проверки) состояния безопасности значимых объектов КИИ; общие требования к созданию системы безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования
		Уметь: определять структуру системы безопасности значимого объекта КИИ; определять требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации; определять требования к обеспечению безопасности значимых объектов КИИ
		Владеть: навыками проведения работ по контролю состояния безопасности объектов КИИ
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств	ОПК-9.1 Проводит анализ профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных	Знать: основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования
		Уметь: определить категорию значимости объектов КИИ
		Владеть: навыками эксплуатации системы безопасности значимого объекта КИИ
	ОПК-9.2 Знает основные информационные технологии, используемые в	Знать: основные принципы выявления наличия критических процессов у субъекта КИИ; основные принципы выявления объектов КИИ, которые

технической защиты информации, сетей и систем передачи информации	автоматизированных системах, их состояние и тенденции развития	обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль и мониторинг критических процессов; процедуры выявления и анализ угроз безопасности информации, обрабатываемой объектом КИИ
		Уметь: определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта КИИ
		Владеть: выявление угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ
	ОПК-9.3 Знает текущее состояние и тенденции развития сетей и систем передачи информации	Знать: общие требования по обеспечению безопасности значимых объектов КИИ; цели, задачи, основные принципы организации государственного контроля области обеспечения безопасности значимых объектов КИИ
		Уметь: определять выбор средств защиты информации с учетом их стоимости, совместимости с применяемыми программными и программное аппаратными средствами, функцией безопасности этих средств и особенностями их реализации, а также категории значимого объекта КИИ
		Владеть: навыками установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ

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. Основы обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ).**						
1.1	Правовые основы обеспечения безопасности КИИ Российской Федерации	7	4	4		6	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3
1.2	Угрозы безопасности информации, обрабатываемой на объектах КИИ	7	6	6		8	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3
2.0	**Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ.**						
2.1	Категорирование объектов КИИ	7	6	6		6	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3
2.2	Требования по обеспечению безопасности значимых объектов КИИ	7	4	4		6	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3
2.3	Система безопасности значимого объекта КИИ	7	4	4		6	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
							ОПК-9.1 ОПК-9.2 ОПК-9.3
2.4	Стадии (этапы) работ по созданию системы безопасности	7	4	4		4	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3
3.0	**Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ.**						
3.1	Контроль за обеспечением безопасности значимого объекта КИИ	7	6	6		4	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3
	Форма промежуточной аттестации – экзамен	7	36				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3
	Итого часов (без учёта часов на промежуточную аттестацию)		34	34		40	

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	А. А. Корниенко, М. А. Еремеев, В. Н. Кустов [и др.] ; под редакцией А. А. Корниенко ; рецензенты : Д. Д. Иванов, В. Ю. Горелик Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте : в 2 частях : учебник / А. А. Корниенко, М. А. Еремеев, В. Н. Кустов [и др.] ; под редакцией А. А. Корниенко ; рецензенты : Д. Д. Иванов, В. Ю. Горелик. Москва : УМЦ ЖДТ, - 448с. - Текст: электронный. - URL: https://umczdt.ru/books/42/30051/	Онлайн
6.1.1.2	Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности:/ Г. Г. Булычев. Москва : РТУ МИРЭА, 2020. - 46с. - Текст: электронный. - URL: https://e.lanbook.com/book/163812 (дата обращения: 19.04.2023)	Онлайн
6.1.1.3	Бутин, А. А. Программно-аппаратные средства защиты информации : учеб. пособие - Изд. 2-е, перераб. и доп. / А. А. Бутин, Н. И. Глухов, С. И. Носков. Иркутск : ИрГУПС, 2022. - 90с.	21
6.1.1.4	Паршин, К. А. Оценка уровня информационной безопасности на объекте информатизации : учеб. пособие для вузов ж.-д. трансп. / К. А. Паршин. М. : УМЦ по образованию на ж.-д. трансп., 2015. - 95с.	17

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз.

		в библиотеке/ онлайн
6.1.2.1	Документальное обеспечение информационной безопасности : учебное пособие для студентов, обучающихся по направлению 10.03.01 «информационная безопасность» / . Севастополь : СевГУ, 2022. - 142с. - Текст: электронный. - URL: https://e.lanbook.com/book/261899 (дата обращения: 19.04.2023)	Онлайн
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Серёдкин, С.П. Методические указания по изучению дисциплины Б1.О.55 Защита объектов критической информационной инфраструктуры по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Безопасность открытых информационных систем / С. П. Серёдкин; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 12 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_8941_1529_2022_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Научная электронная библиотека eLIBRARY.RU — https://elibrary.ru/	
6.2.2	Электронная библиотека Учебно-методического центра по образованию на железнодорожном транспорте «ЭБ УМЦ ЖДТ» — https://umczdt.ru/books/	
6.2.3	Серёдкин С.П. Особенности кибератак на объекты критической информационной инфраструктуры в современных условиях // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2022. – №4(16). – С. 56-66 – DOI: 10.26731/2658-3704.2022.4(16).56-66 – Режим доступа: http://ismm-irgups.ru/toma/416-2022	
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-216 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран,(ноутбук переносной)
3	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран,(ноутбук переносной)
4	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)

5	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Самостоятельная работа	Обучение по дисциплине «Защита объектов критической информационной инфраструктуры» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора.

	Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

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

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

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

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

– самоподготовка и самоконтроль обучающихся в процессе обучения.

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

Для оценки уровня сформированности компетенций используется трехуровневая система:

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

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

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

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

Дисциплина «Защита объектов критической информационной инфраструктуры» участвует в формировании компетенций:

ОПК-5.1. Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

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

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
7 семестр				
1.0	**Раздел 1. Основы обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ)**			
1.1	Текущий контроль	Правовые основы обеспечения безопасности КИИ Российской Федерации	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Конспект (письменно) Собеседование (устно)
1.2	Текущий контроль	Угрозы безопасности информации, обрабатываемой на объектах КИИ	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Конспект (письменно) Реферирование текста (устно/письменно)
2.0	**Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ**			
2.1	Текущий контроль	Категорирование объектов КИИ	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Конспект (письменно)
2.2	Текущий контроль	Требования по обеспечению безопасности значимых объектов КИИ	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Конспект (письменно) Собеседование (устно)
2.3	Текущий контроль	Система безопасности значимого объекта КИИ	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Конспект (письменно)
2.4	Текущий контроль	Стадии (этапы) работ по созданию системы безопасности	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Конспект (письменно) Реферирование текста (устно/письменно)
3.0	**Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ**			
3.1	Текущий контроль	Контроль за обеспечением безопасности значимого объекта КИИ	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Доклад (устно) Конспект (письменно) Собеседование (устно)

			ОПК-9.1 ОПК-9.2 ОПК-9.3	
	Промежуточная аттестация	Раздел 1. Основы обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ). Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ. Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	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	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	Темы конспектов

		оценкой) наиболее ценной (для конспектирующего) информации. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	
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	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	Минимальный

	задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	
«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»	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.Объекты и субъекты. Права и обязанности субъектов КИИ.

2.Полномочия органов государственной власти Российской Федерации в обеспечения безопасности КИИ.

3.Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ.

5.Система безопасности значимого объекта КИИ. Цели и задачи системы безопасности значимого объекта КИИ

6.Права и обязанности субъектов КИИ.

7.Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.

8. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей.

9. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.

10. Правила и порядок категорирования объектов КИИ.

11. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ.

12.Формирование комиссии по категорированию объектов КИИ Российской Федерации.

13.Определение критических процессов в рамках выполнения функций (полномочий) субъекта КИИ.

14.Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управления, контроль и мониторинг критических процессов.

15. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение.

16. Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.

17. Формирования перечня объектов КИИ Российской Федерации, подлежащих категорированию.

18.Порядок определения масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ Российской Федерации.

19.Формирование сведений о результатах категорирования объектов КИИ,

20.Устанеовление требований по обеспечению безопасности значимого объекта КИИ.

21. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ.

22. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ.

23. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ.

24. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ.

25. Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям по безопасности.

26. Требования к созданию систем безопасности значимого объекта КИИ Российской Федерации и обеспечения их функционирования.

27. Требования к силам обеспечения безопасности значимого объекта КИИ.

28.Требования к организационно-распорядительным документам по безопасности значимого объекта КИИ.

29. Перечень необходимых документов в рамках создания систем безопасности значимого объекта КИИ Российской Федерации и обеспечения их функционирования.

30. Этапы жизненного цикла системы безопасности значимого объекта КИИ.

31. Стадии (этапы) работ по созданию системы безопасности значимого объекта КИИ.

32.Внедрение системы безопасности значимого объекта КИИ.

33. Контроль за обеспечением уровня безопасности значимого объекта КИИ.

34.Мониторинг событий безопасности и контроль за действиями персонала значимого объекта КИИ.

35.Оценка соответствия значимых объектов КИИ требованиям безопасности.

36. Документирование процедур и результатов контроля за обеспечением безопасности значимого объекта КИИ.

37. Ответственность за нарушения законодательства о безопасности КИИ Российской Федерации.

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. Объекты и субъекты. Права и обязанности субъектов КИИ.

2.Полномочия органов государственной власти Российской Федерации в обеспечения безопасности КИИ.

3.Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ.

5.Система безопасности значимого объекта КИИ. Цели и задачи системы безопасности значимого объекта КИИ

6.Права и обязанности субъектов КИИ.

7.Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.

8. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей.

9. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.

10. Правила и порядок категорирования объектов КИИ.

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. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ.

2.Формирование комиссии по категорированию объектов КИИ Российской Федерации.

3.Определение критических процессов в рамках выполнения функций (полномочий) субъекта КИИ.

4.Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управления, контроль и мониторинг критических процессов.

5. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение.

6. Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.

7. Формирования перечня объектов КИИ Российской Федерации, подлежащих категорированию.

8.Порядок определения масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ Российской Федерации.

9.Формирование сведений о результатах категорирования объектов КИИ,

10.Устанеовление требований по обеспечению безопасности значимого объекта КИИ.

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. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ.

2. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ.

3. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ.

4. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ.

5. Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям по безопасности.

6. Требования к созданию систем безопасности значимого объекта КИИ Российской Федерации и обеспечения их функционирования.

7. Требования к силам обеспечения безопасности значимого объекта КИИ.

8.Требования к организационно-распорядительным документам по безопасности значимого объекта КИИ.

9. Перечень необходимых документов в рамках создания систем безопасности значимого объекта КИИ Российской Федерации и обеспечения их функционирования.

10. Этапы жизненного цикла системы безопасности значимого объекта КИИ.

11. Стадии (этапы) работ по созданию системы безопасности значимого объекта КИИ.

12.Внедрение системы безопасности значимого объекта КИИ.

13. Контроль за обеспечением уровня безопасности значимого объекта КИИ.

14.Мониторинг событий безопасности и контроль за действиями персонала значимого объекта КИИ.

15.Оценка соответствия значимых объектов КИИ требованиям безопасности.

16. Документирование процедур и результатов контроля за обеспечением безопасности значимого объекта КИИ.

17. Ответственность за нарушения законодательства о безопасности КИИ Российской Федерации.

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-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Правовые основы обеспечения безопасности КИИ Российской Федерации	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Угрозы безопасности информации, обрабатываемой на объектах КИИ	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 3 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Категорирование объектов КИИ	Знание	4 – ОТЗ 3 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 3 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Требования по обеспечению безопасности значимых объектов КИИ	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	3 – ОТЗ 3 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Система безопасности значимого объекта КИИ	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Стадии (этапы) работ по созданию системы безопасности	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-9.1 ОПК-9.2 ОПК-9.3	Контроль за обеспечением безопасности значимого объекта КИИ	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.

1. Безопасность критической информационной инфраструктуры:

а) состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак

б) обеспечение безопасного уровня защиты информации для обеспечения устойчивого функционирования критической информационной инфраструктуры

в) состояние защиты информации критической информационной инфраструктуры обеспечивающее её устойчивое функционирование.

2. Значимый объект критической информационной инфраструктуры:

Ответ: объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

3. Объекты критической информационной инфраструктуры:

а) объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия с автоматизированными системами управления;

б) объекты информационной инфраструктуры, прошедшие процедуру категорирования;

в) информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

4. Принципами обеспечения безопасности критической информационной инфраструктуры являются:

а) законность, непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;

б) приоритет предотвращения компьютерных атак, законность;

в) законность, непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры, приоритет предотвращения компьютерных атак.

5. Категорирование объекта критической информационной инфраструктуры:

а) процедура установления объекту критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения;

б) установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений;

в) установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

6. Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:

а) предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления

и распространения, а также иных неправомерных действий в отношении такой информации;

б) недопущение воздействия на технические средства обработки информации, обеспечение функционирования значимого объекта критической информационной инфраструктуры;

в) восстановление функционирования значимого объекта критической информационной инфраструктуры.

7. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение:

а) отсутствие доступа к государственной услуге в течении, которого государственная услуга может быть недоступна для получателей;

б) причинение ущерба жизни и здоровью людей;

в) прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны.

8. Максимальный срок категорирования не должен превышать;

Ответ: одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения дополнений, изменений);

9. Создание и функционирование систем безопасности должно быть направлено на:

а) обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак;

б) обеспечение защиты значимых объектов критической информационной инфраструктуры от компьютерных атак;

в) обеспечение функционирования значимых объектов критической информационной инфраструктуры при возникновении угроз информационной безопасности.

10. Системы безопасности должны обеспечивать:

Ответ: устойчивое функционирование системы безопасности значимых объектов критической информационной инфраструктуры.

11. К силам обеспечения безопасности значимых объектов критической информационной инфраструктуры относятся:

Ответ: подразделения (работники) субъекта критической информационной инфраструктуры, ответственные за обеспечение безопасности значимых объектов критической информационной инфраструктуры;

12. Организационно-технические меры по обеспечению безопасности значимого объекта должны включать:

Ответ: анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);

б) разработку технического задания на создание системы безопасности значимого объекта;

в) разработку рабочей (эксплуатационной) документации на систему защиты

13. Модель угроз безопасности информации должна содержать:

а) краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта;

б) модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта;

в) краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации.

14. Кем осуществляется государственный контроль за обеспечением уровня безопасности значимого объекта КИИ:

Ответ: ФСТЭК.

15. Ответственность за нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

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

16. Исходя из каких параметров осуществляется категорирование объекта КИИ?

Ответ: социальной значимости, политической значимости, экономической значимости, экологической значимости, значимости для обеспечения обороны страны.

17. В отношении каких объектов КИИ должны создаваться системы безопасности?

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

18. Каким документом оформляется решение комиссии по категорированию объекта КИИ?

Ответ: Решение комиссии по категорированию оформляется актом.

3.6 Перечень теоретических вопросов к экзамену

(для оценки знаний)

1. Объекты и субъекты. Права и обязанности субъектов КИИ.
2.Полномочия органов государственной власти Российской Федерации в обеспечения безопасности КИИ.
3.Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ.
5.Система безопасности значимого объекта КИИ. Цели и задачи системы безопасности значимого объекта КИИ
6.Права и обязанности субъектов КИИ.
7.Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.
8. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей.
9. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.
10. Правила и порядок категорирования объектов КИИ.
11. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ.
12.Формирование комиссии по категорированию объектов КИИ Российской Федерации.
13.Определение критических процессов в рамках выполнения функций (полномочий) субъекта КИИ.
14.Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управления, контроль и мониторинг критических процессов.
15. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение.
16. Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.
17. Формирования перечня объектов КИИ Российской Федерации, подлежащих категорированию.
18.Порядок определения масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ Российской Федерации.
19.Формирование сведений о результатах категорирования объектов КИИ,
20.Устанеовление требований по обеспечению безопасности значимого объекта КИИ.
21. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ.
22. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ.

23. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ.
24. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ.
25. Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям по безопасности.
26. Требования к созданию систем безопасности значимого объекта КИИ Российской Федерации и обеспечения их функционирования.
27. Требования к силам обеспечения безопасности значимого объекта КИИ.
28.Требования к организационно-распорядительным документам по безопасности значимого объекта КИИ.
29. Перечень необходимых документов в рамках создания систем безопасности значимого объекта КИИ Российской Федерации и обеспечения их функционирования.
30. Этапы жизненного цикла системы безопасности значимого объекта КИИ.
31. Стадии (этапы) работ по созданию системы безопасности значимого объекта КИИ.
32.Внедрение системы безопасности значимого объекта КИИ.
33. Контроль за обеспечением уровня безопасности значимого объекта КИИ.
34.Мониторинг событий безопасности и контроль за действиями персонала значимого объекта КИИ.
35.Оценка соответствия значимых объектов КИИ требованиям безопасности.
36. Документирование процедур и результатов контроля за обеспечением безопасности значимого объекта КИИ.
37. Ответственность за нарушения законодательства о безопасности КИИ Российской Федерации.

3.7 Перечень типовых простых практических заданий к экзамену

(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. Дать характеристики программы поиска и гарантированного уничтожения информации на дисках
2. Перечислить возможности средств анализа и контроля защищенности информации (сетевые сканеры).
3. Подготовить схему технической защиты локальной сети объекта КИИ.

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 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

ИРГУПС 20__-20__ учебный год	**Экзаменационный билет № 1** **по дисциплине «Защита объектов критической информационной инфраструктуры»**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____
1.Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение. 2.Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности. 3.Формирования перечня объектов КИИ Российской Федерации, подлежащих категорированию. Практический вопрос: 1.Подготовить схему технической защиты локальной сети объекта КИИ.		