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.07 Информационная безопасность критической информационной инфраструктуры

рабочая программа дисциплины

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

Общая трудоемкость в з.е. – 3
Часов по учебному плану (УП) – 108

Формы промежуточной аттестации
очная форма обучения:
экзамен 1 семестр

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

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

ИРКУТСК

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

Программу составил(и):
к.э.н., доцент, 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 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цель дисциплины	
1	формирование у студентов системных знаний по обеспечению информационной безопасности критической информационной инфраструктуры, а также 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	изучения 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

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	Дисциплина изучается на начальном этапе формирования компетенции
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
2	Б3.02(Д) Защита выпускной квалификационной работы

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1 Знает основные виды организационно-распорядительных документов в области ИБ, требования по формированию политик ИБ, защите компьютерных систем и сетей	Знать: нормативно правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ; 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; 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; обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ
		Владеть: навыками работы с нормативно правовыми актами, методическими документами и национальными стандартами в области обеспечения безопасности значимых объектов КИИ; 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 эксплуатации системы безопасности значимого объекта КИИ

	ОПК-3.2 Умеет разрабатывать организационно-распорядительные документы и формировать политику в области информационной безопасности	Знать: основные принципы выявления наличия критических процессов у субъекта КИИ; основные принципы выявления объектов КИИ, которые 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; общие требования по обеспечению безопасности значимых объектов КИИ; цели, задачи, основные принципы организации государственного контроля области обеспечения безопасности значимых объектов КИИ
		Уметь: определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта КИИ; 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 выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ; 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 КИИ.**						
1.1	Правовые основы обеспечения безопасности КИИ Российской Федерации	1	2	6		3	ОПК-3.1
1.2	Угрозы безопасности информации, обрабатываемой на объектах КИИ	1	3	4		3	ОПК-3.1 ОПК-3.2
2.0	**Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ.**						
2.1	Категорирование объектов КИИ	1	2	4		3	ОПК-3.1 ОПК-3.2
2.2	Требования по обеспечению безопасности значимых объектов КИИ	1	2	6		3	ОПК-3.1 ОПК-3.2
2.3	Система безопасности значимого объекта КИИ	1	4	4		3	ОПК-3.1 ОПК-3.2
2.4	Стадии (этапы) работ по созданию системы безопасности	1	2	6		3	ОПК-3.1 ОПК-3.2
3.0	**Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ.**						
3.1	Контроль за обеспечением безопасности значимого объекта КИИ	1	2	4		3	ОПК-3.1
	Форма промежуточной аттестации – экзамен	1	36				
	Итого часов (без учёта часов на промежуточную аттестацию)		17	34		21	

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	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
6.1.1.3	Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 195с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=208567 (дата обращения: 14.09.2022)	Онлайн
6.1.1.4	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : учеб. пособие / В. Ф. Шаньгин. М. : ДМК, 2008. - 542с.	30

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
6.1.2.2	Информационная безопасность цифровой экономики. Материалы XVII научно-теоретической конференции VIII Пленума регионального отделения Федерального учебнометодического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» по Сибирскому и Дальневосточному федеральным округам (СибРОУМО), 13 октября – 15 октября 2021 г. : материалы конференции / . Новосибирск : СибГУТИ, 2021. - 124с. - Текст: электронный. - URL: https://e.lanbook.com/book/257252 (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.07 Информационная безопасность критической информационной инфраструктуры по направлению подготовки 10.04.01 Информационная безопасность, профиль Безопасность информационных систем и технологий /к.э.н. С.П. Серёдкин; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 11 с - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_10610_1506_2022_1_signed.pdf	Онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»

6.3 Программное обеспечение и информационные справочные системы

6.3.1 Базовое программное обеспечение

6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/

6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License
6.3.2 Специализированное программное обеспечение	
6.3.2.1	Не предусмотрено
6.3.3 Информационные справочные системы	
6.3.3.1	Не предусмотрены
6.4 Правовые и нормативные документы	
6.4.1	Не предусмотрены

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

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

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

	детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
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 «Информационная безопасность 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 «Информационная безопасность критической информационной инфраструктуры» участвует в формировании компетенций:

ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
1 семестр				
1.0	**Раздел 1. Основы обеспечения безопасности значимых объектов КИИ**			
1.1	Текущий контроль	Правовые основы обеспечения безопасности КИИ Российской Федерации	ОПК-3.1	Конспект (письменно). Собеседование (устно
1.2	Текущий контроль	Угрозы безопасности информации, обрабатываемой на объектах КИИ	ОПК-3.1 ОПК-3.2	Конспект (письменно). Собеседование (устно
2.0	**Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ**			
2.1	Текущий контроль	Категорирование объектов КИИ	ОПК-3.1 ОПК-3.2	Конспект (письменно). Собеседование (устно
2.2	Текущий контроль	Требования по обеспечению безопасности значимых объектов КИИ	ОПК-3.1 ОПК-3.2	Конспект (письменно). Доклад
2.3	Текущий контроль	Система безопасности значимого объекта КИИ	ОПК-3.1 ОПК-3.2	Конспект (письменно). Собеседование (устно
2.4	Текущий контроль	Стадии (этапы) работ по созданию системы безопасности	ОПК-3.1 ОПК-3.2	Конспект (письменно). Собеседование (устно
3.0	**Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ**			
3.1	Текущий контроль	Контроль за обеспечением безопасности значимого объекта КИИ	ОПК-3.1	Конспект (письменно) Доклад
	Промежуточная аттестация		ОПК-3.1 ОПК-3.2	Экзамен (собеседование) Экзамен - тестирование (компьютерные технологии)

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

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

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

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки.

Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

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

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

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы по темам/разделам дисциплины
2	Конспект	Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор реферата раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Может быть использовано для оценки знаний и умений обучающихся	Вопросы по темам/разделам дисциплины
3	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, сообщений

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (образец экзаменационного билета) к экзамену
2	Тест – промежуточная аттестация в форме экзамена	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

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

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

Тест – промежуточная аттестация в форме экзамена

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

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

3.1 Типовые контрольные вопросы для подготовки доклада

3.1 Типовые контрольные задания

3.1.1 Собеседование

Собеседование с обучающимися проходит на семинарских занятиях. В момент проведения собеседования пользоваться учебниками, справочниками, конспектами лекций запрещено.

Преподаватель заранее оглашает учащимся перечень вопросов, ответы на которые необходимо подготовить учащимся самостоятельно.

Задачи проведения собеседования с обучающимися:

– проверка и контроль полученных знаний по изученной теме;

– расширение проблематики в рамках дополнительных вопросов по изученной теме;

– углубление знаний;

– формирование навыков беседы, декларирования знаний и рассуждения.

Перечень вопросов:

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.

Критерии и шкала оценивания собеседования

Оценка	Критерий оценки
«отлично»	Дан полный ответ на предложенный вопрос (обучающийся владеет терминологией, умеет анализировать и рассуждать). Даны правильные ответы на дополнительные вопросы преподавателя в рамках рассматриваемого вопроса, приведены примеры.
«хорошо»	Дан полный ответ на предложенный вопрос (обучающийся владеет терминологией, умеет анализировать и рассуждать). Частично даны правильные ответы на дополнительные вопросы преподавателя в рамках рассматриваемого вопроса, не приведены примеры.
«удовлетворительно»	Полные ответы на предложенные вопросы не даны (приведены только определения основных терминов).
«неудовлетворительно»	Учащийся не смог ответить на поставленные вопрос и дополнительные вопросы по заданной теме.

3.1.2 Доклад, сообщение

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 доклада, сообщения:

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.

Критерии и шкала оценивания

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	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»	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 сообщения не передана

3.2 Перечень теоретических вопросов к экзамену

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.

3.3 Типовые контрольные задания для проведения тестирования

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

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ПК-1.2	Тема 1. Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления.	Знание	2 – ОТЗ 8 – ЗТЗ
ПК-1.2	Тема 2. Идентификация активов (описание бизнес-процессов).	Знание	9 – ОТЗ 8 – ЗТЗ
ПК-1.2	Тема 3. Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками.	Знание	9 – ОТЗ 8 – ЗТЗ
		Умение	10 – ОТЗ 10 – ЗТЗ
ПК-1.2	Тема 4. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	Знание	9 – ОТЗ 8 – ЗТЗ
		Умение	10 – ОТЗ 10 – ЗТЗ

ПК-1.2	Тема 5. Системный подход к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками, деятельности по управлению рисками (сопровождение и мониторинг механизмов безопасности, пересмотр и переоценка риска, управление документами и записями, корректирующие и превентивные меры, коммуникация рисков). Аутсорсинг процессов управления рисками. Распределение ответственности за управление рисками.	Знание	9 – ОТЗ 8 – ЗТЗ
ПК-1.2	Тема 6. Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками.	Знание	9 – ОТЗ 8 – ЗТЗ
		Умение	10 – ОТЗ 10 – ЗТЗ
ПК-1.2	Тема 7. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы.	Знание	9 – ОТЗ 8 – ЗТЗ
		Умение	10 – ОТЗ 10 – ЗТЗ
ПК-1.2	Тема 8. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	Знание	9 – ОТЗ 8 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 6 – ЗТЗ
ПК-1.2	Тема 9. Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность.	Знание	9 – ОТЗ 8 – ЗТЗ
		Умение	10 – ОТЗ 10 – ЗТЗ
		Итого	60

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:

а), объект критической информационной инфраструктуры который включен в в реестр значимых объектов критической информационной инфраструктуры;

б). объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

в). объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости

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;

3) 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;

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

б). двух лет со дня утверждения субъектом критической информационной инфраструктуры перечня объектов (внесения дополнений, изменений);

в). 6 месяцев 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:

а). восстановление функционирования системы безопасности значимых объектов критической информационной инфраструктуры;

б). недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов критической информационной инфраструктуры

в). устойчивое функционирование системы безопасности значимых объектов критической информационной инфраструктуры.

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

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

б). подразделения (работники), участвующие в подготовке плана безопасности значимого объекта критической информационной инфраструктуры.

в). подразделения (работники), эксплуатирующие значимые объекты критической информационной инфраструктуры.

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

а). 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). числе 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 осуществляет;

а). ФСБ;

б). ФСТЭК;

в). Органами прокуратуры РФ.

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

а). дисциплинарная;

б). дисциплинарная и административная;

в). дисциплинарная, гражданско-правовая, административная и уголовная ответственность.

16. Риск информационной безопасности:

А) Потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации;

Б) Вероятные потери организации в результате инцидентов;

В) Возможность минимизации угрозы информационной безопасности.

17. Основными источниками угроз информационной безопасности являются все указанное в списке:

А) Хищение жестких дисков, подключение к сети, инсайдерство

Б) Перехват данных, хищение данных, изменение архитектуры системы

В) Хищение данных, подкуп системных администраторов, нарушение регламента работы.

18. Алгоритм оценки имеющихся корпоративных информационных активов включает в себя их описание по следующим категориям:

А) Человеческие ресурсы (надежность персонал), информационные активы;

Б) Сервисные ресурсы, помещения, в которых обрабатывается, хранится информация;

В) Программные ресурсы, физические ресурсы (сервера, рабочие станции, сетевое и телекоммуникационное оборудование).

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

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 2022-2023 учебный год	**Экзаменационный билет № 1** **по дисциплине «Информационная безопасность критической информационной инфраструктуры»**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____**Т.К. Кириллова.**
1.Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значение. 2.Требования к силам обеспечения безопасности значимого объекта КИИ. 3. Объекты и субъекты. Права и обязанности субъектов КИИ		