ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказ ректора
от «07» июня 2021 г. № 78

Б1.О.55 Защита объектов критической информационной инфраструктуры

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – N 5 "Безопасность открытых информационных систем"
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – 5лет 6м., очная форма
Кафедра-разработчик программы – Информационные системы и защита информации

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

Формы промежуточной аттестации в семестрах
экзамен - 7

Распределение часов дисциплины по семестрам

Семестр	7	**Итого**
Число недель в семестре	16	
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)	34/4	34/4
– лабораторные	-	-
Самостоятельная работа	**40**	**40**
Экзамен	**36**	**36**
Итого	**144**	**144**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

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

Программу составил:
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 «04» 06 2021 г. № 11/2

И.о.зав. кафедрой «ИСиЗИ» Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели дисциплины	
1	Целями освоения дисциплины являются 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	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.
	1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины
	Цель воспитания обучающихся – разностороннее развитие личности будущего конкурентоспособного специалиста с высшим образованием, обладающего высокой культурой, интеллигентностью, социальной активностью, качествами гражданина-патриота. Задачи воспитательной работы с обучающимися: – развитие мировоззрения и актуализация системы базовых ценностей личности; – приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям; – воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности как важнейшей черты личности, проявляющейся в заботе о своей стране, сохранении человеческой цивилизации; – воспитание положительного отношения к труду, развитие потребности к творческому труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях; – обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности; – выявление и поддержка талантливых обучающихся, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
Данной дисциплине предшествует дисциплины: - Б1. О.48 Теоретические основы компьютерной безопасности; - Б1. О.37 Защита информации от утечки по техническим каналам; - Б1. О.30 Безопасность операционных систем; - Б2.В.01(П) Производственная - технологическая практика	
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.41 Управление информационной безопасностью
2	Б1.О.39 Программно-аппаратные средства защиты информации
3	Б1.О.32 Безопасность систем баз данных
4	Б1.В.ДВ.04.01 Защита электронного документооборота
5	Б2.В.02(П) Производственная - эксплуатационная

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-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;	ОПК-9.1Проводит анализ профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных ОПК-9.2Знает основные информационные технологии, используемые в автоматизированных системах, их состояние и тенденции развития ОПК-9.3Знает текущее состояние и тенденции развития сетей и систем передачи информации	**Знать:** основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования; 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:** определить категорию значимости объектов КИИ; 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:** эксплуатации системы безопасности значимого объекта КИИ; выявление угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ; установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ;
ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых	ОПК-5.1.1Знает особенности разработки политики информационной безопасности открытых информационных систем ОПК-5.1.2Умеет формировать исходные требования для разработки политики	**Знать**: нормативно правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ; процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ;

информационных систем	информационной безопасности ОПК-5.1.3Имеет навыки обоснования целесообразности реализации политики информационной безопасности открытых информационных систем	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; 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:** 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; формировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий; определять структуру системы безопасности значимого объекта КИИ; определять требования к параметрам настройки программных и программное 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**: работы с нормативно правовыми актами, методическими документами и национальными стандартами в области обеспечения безопасности значимых объектов КИИ; работы с базами данных, содержащую информацию по угрозам безопасности информации м уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными

		ресурсами; разработки организационно-распорядительных документов по безопасности значимых объектов КИИ; участия в разработке организационных и технических мероприятий по защите объектов КИИ; проведения работ по контролю состояния безопасности объектов КИИ.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работы	Семестр	Часы				*Код индикатора достижения компетенции
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Основы обеспечения безопасности значимых объектов КИИ**	7					
1.1	Правовые основы обеспечения безопасности КИИ Российской Федерации (Лек,Пр)		4	4		6	ОПК-5.1 ОПК-9
1.2	Угрозы безопасности информации, обрабатываемой на объектах КИИ (Лек,Пр)		6	6		8	ОПК-5.1 ОПК-9
2.0	**Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ**	7					
2.1	Категорирование объектов КИИ		6	6		6	ОПК-5.1 ОПК-9
2.2	Требования по обеспечению безопасности значимых объектов КИИ (Лек,Пр)		4	4		6	ОПК-5.1 ОПК-9
2.3	Система безопасности значимого объекта КИИ (Лек,Пр)		4	4		6	ОПК-5.1 ОПК-9
2.4	Стадии (этапы) работ по созданию системы безопасности (Лек,Пр)		4	4		4	ОПК-5.1 ОПК-9
3.0	**Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ**	7					
3.1	Контроль за обеспечением безопасности значимого объекта КИИ (Лек,Пр)		6	6		4	ОПК-5.1 ОПК-9
4.0	**Раздел 4 .Экзамен**	7				36	
4.1	Завершающий экзамен по курсу /Экзамен/						ОПК-5.1 ОПК-9

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

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.1	К. А. Паршин.	Оценка уровня информационной безопасности на объекте информатизации учеб. пособие для вузов ж.-д. транспорта. https://www.studmed.ru/	Учеб. пособие. — М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2015.	100% онлайн

6.1.2	И.А.Трещев	Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте https://search.rsl.ru/	Москва : Учебно-методический центр по образованию на ж.-д. трансп., 2014	100% онлайн
6.1.3	В.Ф.Шаньгин	Защита компьютерной информации. Эффективные методы и средства https://avidreaders.ru/book/	Москва: ДМК Пресс. 2010	100% онлайн
6.1.4	А.А.Титов	Инженерно-техническая защита информации. Учебное пособие	Москва : ДМК Пресс, 2010	100% онлайн
6.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.2.1	С.В. Петров	Информационная безопасность: учеб. пособие. https://www.yandex.ru/search/direct	Москва : АРТА, 2012.	100% онлайн
6.1.2.2	А. С. Олейник	Моделирование безопасности и защищенности критически важных объектов, научная статья. https://elibrary.ru/item.asp?id=29881512	Москва: Железнодорожный транспорт. - 2017. - № 9.	100% онлайн
6.1.2.3.	Д. Костров	Костров, Дмитрий. Как защитить критически важные объекты? научная статья https://www.secuteck.ru/contacts?hsCtaTracking=6936445	Москва: Системы безопасности. 2015, -№2	100% онлайн
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
6.1.3.1	А.А. Бутин	Методы и средства защиты информации от несанкционированного доступа. Программно-аппаратный уровень: учеб. пособие http://www.irgups.ru/ntb//Jirbis/index.php?option	Иркутск: ИрГУПС, 2015	100% онлайн
6.1.3.2	В.В.Креопалов	Технические средства и методы защиты информации. Технические средства и методы защиты информации. Учебно-практическое пособие. https://search.rsl.ru/ru/record/01006553324	Москва : Евразийский открытый ин-т, 2011	100% онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»				
6.2.1	Сайт ФСТЭК РФ http://fstec.ru/			

6.2..2	Сайт ФСБ РФ http://www.fsb.ru/
6.2.3	Сайт производителя Dr. Web Cureit! http://free.drweb.ru/
6.2.4	Сайт «Код безопасности» http://www.securitycode.ru
6.2.5	Сайт производителя Acronis http://www.acronis.com/ru-ru/
6.2.6	Сайт производителя 360 Total Security http://360-total-security.besplatnyeprogrammy.ru/
6.2.7	Сайт производителя Dallas Lock https://www.dallaslock.ru/
6.2.8	Сайт производителя линейки «ViPNet» http://www.infotecs.ru/
6.2.9	Сайт производителя ruToken http://www.rutoken.ru/
6.2.10	Искусство управления информационной безопасностью http://www.iso27000.ru
6.2.11	DLP-системы https://www.infowatch.ru/dlp
6.2.12	Материалы «Комплексная защита информации в компьютерных системах» /http://padaread.com
6.3 Программное обеспечение и информационные справочные системы	
6.3.1 Базовое программное обеспечение	
6.3.1.1	ОС Microsoft Windows 7 Professional, количество – 100, лицензия № 49379844, обновление - Контракт № 0334100010016000113-0000756-02 от 25.11.2016г., обновление - договор №31705062861 от 06.06.2017 АО СофтЛайнТрейд, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд
6.3.1.2	Офисный пакет Microsoft Office 2010, количество – 155, Лицензия № 48288083, обновление - Контракт № 0334100010016000113-0000756-02 от 25.11.2016г., обновление - договор №31705062861 от 06.06.2017 АО СофтЛайнТрейд, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org
6.3.2 Специализированное программное обеспечение	
6.3.2.1	Сканер MBSA (свободное ПО);
6.3.2.2	«Сканер-ВС» (свободное ПО для вузов);
6.3.2.3	СЗИ от НСД SecretNet (лицензия);
6.3.2.4	Персональные идентификаторы ruToken;
6.3.2.5	Электронный замок Соболь-PCI;
6.3.2.6	СЗИ НСД Dallas Lock (свободное ПО для вузов);
6.3.2.7	Пакет PrZamena (свободное ПО);
6.3.2.8	Dr.Web Cureit! (свободное ПО);
6.3.2.9	360 Total Security (свободное ПО).
6.3.3 Информационные справочные системы	
6.3.3.1	КонсультантПлюс – студенческая версия (Онлайн–версия КонсультантПлюс: Студент, https://student2.consultant.ru/cgi/online.cgi?req=home;rnd=0.8160556428138959)
6.4Правовые и нормативные документы	
6.4.1	Закон Российской Федерации от 21 июня 1993г. №5485-1 «О государственной тайне».
6.4.2	Федеральный закон от 26 июня 2017г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6.4.3	Федеральный закон от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
6.4.4	Федеральный закон от 04 мая 2011г. №99-ФЗ «О лицензировании отдельных видов деятельности».
6.4.5	Федеральный закон от 29 июня 2015г. №162-ФЗ «О стандартизации отдельных видов деятельности».
6.4.6	Перечень сведений, отнесенных к государственной тайне. Утвержден указом Президента Российской Федерации от 30 ноября 1995г. №1203.
6.4.7	Правила категорирования объектов критической инфраструктуры Российской Федерации. Утверждены Постановлением Правительства Российской Федерации от 08 февраля 2018г. №127.
6.4.8	Требования к созданию систем безопасности значимых объектов критической инфраструктуры Российской Федерации и обеспечения их функционирования. Утверждены приказом ФСТЭК России от 21 декабря 2017г. №235.

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 – по адресу г. Иркутск, ул. Лермонтова, д.80.
2	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации, плакаты, таблицы), обеспечивающие тематические иллюстрации содержания дисциплины:Д-518,521,623,Д-216.
3	Учебная лаборатория «Информационной безопасности транспортной инфраструктуры» -Д-525. Оснащение лаборатории: Автоматизированное рабочее место преподавателя в составе: ПЭВМ, Принтер LCD. Операционная система. Офисные программы. Антивирусные программы. Автоматизированное рабочее место обучавшегося (в расчете – одно рабочее место на одного обучающегося) в составе: ПЭВМ. Операционная система. Офисные программы. Антивирусные программы. Программное обеспечение для проведения компьютерных тестов. Учебные лабораторные комплексы для: Контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры; Проведения анализа защищённости значимого объекта КИИ на соответствие требованиям по обеспечению безопасности.
4	Помещения для самостоятельной работы обучающихся: – Читальный зал А-606. Учебная мебель, стеллажи, витрина, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, мультимедийный проектор, экран. – Аудитория Д-523,508,514. Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, мультимедийный проектор, экран.
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.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	
Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. 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	Обсуждение лекционного материала и материала, выносимого на самостоятельное изучение, закрепление изученного материала при помощи выполнения различных практических заданий.
Самостоятельная работа	Самостоятельная работа обучающихся проводится в целях закрепления и систематизации теоретических знаний, а также формирования практических навыков по их применению при решении прикладных задач в выбранной предметной области. Она включает проработку лекционного материала, самоподготовку обучающихся к практическим занятиям, выполнение практических задач, самостоятельное изучение тем, выходящих за рамки лекционного курса.
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.	

Лист регистрации дополнений и изменений рабочей программы дисциплины

№ п/п	Часть текста, подлежавшего изменению в документе			Общее количество страниц		Основание для внесения изменения, № документа	Подпись отв. исп.	Дата
	№ раздела	№ пункта	№ подпункта	до внесения изменений	после внесения изменений			

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.О.55 Информационная безопасность критической информационной инфраструктуры

Приложение № 1 к рабочей программе

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – №5 "Безопасность открытых информационных систем"

ИРКУТСК

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 Университета, 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.

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.О.55 Информационная безопасность критической информационной инфраструктуры прошел экспертизу на соответствие требованиям ФГОС по направлению 10.05.03 Безопасность информационных систем и технологий (специалист по защите информации), рассмотрен и рекомендован к внедрению на заседании СОП по специальности № 5 "Безопасность открытых информационных систем".

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

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

Программа контрольно-оценочных мероприятий очная форма обучения

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятие/тем/раздел и т.д. дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
7 семестр					
1.	1.2	Текущий контроль	Правовые основы обеспечения безопасности КИИ Российской Федерации	ОПК-9 ОПК-5.1	Конспект (письменно). Собеседование (устно
2.	3.4	Текущий контроль	Угрозы безопасности информации, обрабатываемой на объектах КИИ	ОПК-9 ОПК-5.1	Конспект (письменно).
3.	5.6	Текущий контроль	Категорирование объектов КИИ	ОПК-9 ОПК-5.1	Конспект (письменно). Компьютерные технологии.
4.	7.8	Текущий контроль	Требования по обеспечению безопасности значимых объектов КИИ	ОПК-9 ОПК-5.1	Конспект (письменно). Собеседование (устно
5.	9.10	Текущий контроль	Система безопасности значимого объекта КИИ	ОПК-9 ОПК-5.1	Конспект (письменно) Компьютерные технологии.
6.	11.12	Текущий контроль	Стадии (этапы) работ по созданию системы безопасности	ОПК-9 ОПК-5.1	Конспект (письменно).
7.	13.14. 15	Текущий контроль	Контроль за обеспечением безопасности значимого объекта КИИ	ОПК-9 ОПК-5.1	Конспект (письменно). Собеседование (устно
8.	16	Промежуточный контроль – экзамен	Раздел 1. Основы обеспечения безопасности значимых объектов КИИ Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ	ОПК-9 ОПК-5.1	Тест

Описание показателей и критериев оценивания компетенций. Описание шкал оценивания

Контроль качества освоения дисциплины/прохождения практики 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/или двухбалльная шкала: «зачтено», «не зачтено».

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

№	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	Реферат	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	Темы рефератов
3	Сообщение, 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
4	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	Тест

Критерии и шкалы оценивания компетенций в результате изучения дисциплины «Защита объектов критической информационной инфраструктуры» при проведении промежуточной аттестации в форме экзамена. Шкала оценивания уровня освоения компетенций

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»		Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»		Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного	Минимальный

		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	
«неудовлетворительно»	«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкала оценивания	Критерии оценивания
«отлично»	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 было попытки выполнить задание

Реферат

Шкала оценивания	Критерии оценивания
«отлично»	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы
«хорошо»	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы
«удовлетворительно»	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод
«неудовлетворительно»	Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы. Реферат обучающимся не представлен

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

Оценочное средство «Тест».

Тестирование с применением компьютерных технологий проводится по окончанию изучения дисциплины и (или) в течение года по завершению изучения дисциплины (контроль/проверка остаточных знаний, умений, навыков и (или) опыта деятельности).

Тесты формируются из фонда тестовых заданий по дисциплине. Структура фонда тестовых заданий по дисциплине, структуры тестов итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа.

Результаты тестирования могут быть использованы при проведении промежуточной аттестации в форме экзамена.

Промежуточная аттестация в форме экзамена – результаты тестирования могут являться допуском к экзамену:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	Обучающийся к экзамену допущен
Обучающийся набрал при тестировании менее 69 баллов	Обучающийся к экзамену не допущен

Преподаватель вправе предусмотреть тесты для самоконтроля обучающихся по разделам дисциплины, сформировав их из материалов фонда тестовых заданий дисциплины. Требования к тестам для самоконтроля аналогичны требованиям к итоговым тестам по семестрам и дисциплине в целом.

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

3.1 Типовые темы для контрольных заданий 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 темы рефератов

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

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

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

4. Правила и порядок категорирования объектов КИИ.

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

6.Формирование комиссии по категорированию объектов КИИ Российской Федерации.

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

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

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

1.Устанеовление требований по обеспечению безопасности значимого объекта КИИ.

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

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

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

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

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

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

17. Требования к силам обеспечения безопасности значимого объекта КИИ.

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

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

20. Этапы жизненного цикла системы безопасности значимого объекта КИИ.

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

22.Внедрение системы безопасности значимого объекта КИИ.

23. Контроль за обеспечением уровня безопасности значимого объекта КИИ.

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

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

26.Оценка соответствия значимых объектов КИИ требованиям безопасности.

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

3.3 Типовые темы докладов, сообщений

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.

3.4 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.

3.5 Перечень типовых простых практических заданий к экзамену

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

3.6 Тестирование по дисциплине

3.6.1. Структура фонда тестовых заданий по дисциплине

Структура фонда тестовых заданий по дисциплине «Защита объектов критической информационной инфраструктуры»

Раздел дисциплины	Количество ТЗ, типы ТЗ
Раздел 1. 1. Основы обеспечения безопасности значимых объектов КИИ	10 – тип А 10 - тип В 10 – тип С

	6 – тип D
Итого по разделу	**$\sum$ 36** **10 – тип А** **10-тип В** **10 – тип С** **6 – тип D**
Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ	20 – тип А 10 - тип В 3 – тип С 3 – тип D
Итого по разделу	**$\sum$ 36** **20– тип А** **10 - тип В** **3 – тип С** **3 – тип D**
Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ	20 – тип А 10 - тип В 3 – тип С 3 – тип D
Итого по разделу	**20 – тип А** **10 - тип В** **3 – тип С** **3 – тип D**
Итого по дисциплине	**$\sum$ 108** **50– тип А** **30 - тип В** **16– тип С** **912– тип D**

Используемые типы тестовых заданий (ТЗ):

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

ТЗ типа В: тестовое задание открытой формы (с конструируемым ответом: ТЗ с кратким регламентируемым ответом (ТЗ дополнения); ТЗ свободного изложения (с развернутым ответом в произвольной форме);

ТЗ типа С: тестовое задание на установление соответствия;

ТЗ типа Д: тестовое задание на установление правильной последовательности.

3.6.2. Структура и образец типового теста за 7 семестр по дисциплине за весь период ее освоения

Раздел дисциплины	Количество ТЗ, типы ТЗ
Раздел 1. Основы обеспечения безопасности значимых объектов КИИ	3 – тип А 2 – тип В 1 – тип С
Итого по разделу	**$\sum$ 6** **3 – тип А** **2 – тип В** **1 – тип С**
Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ	2 – тип А 2 – тип В 1 – тип С 1 – тип D
Итого по разделу	**$\sum$ 6** **2 – тип А** **2 – тип В** **1 – тип С** **1 – тип D**

Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ	1 – тип А 1- тип В 1 – тип С 3
Итого по разделу	**∑ 3** **1 – тип А** **1– тип В** **1 – тип С**
Итого по дисциплине	**∑ 15** **6 – тип А** **5 – тип В** **3 – тип С** **1 – тип D**

Образец типового теста
за 7 семестр по дисциплине за весь период ее освоения

Описание требований к тесту: итоговый тест по дисциплине «Защита объектов критической информационной инфраструктуры»:

- знает: основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования; 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;
- умеет: определить категорию значимости объектов КИИ; 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;
- владеет навыками: эксплуатации системы безопасности значимого объекта КИИ; выявление угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ; установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ.

Студенту необходимо выполнить 60 тестовых заданий. Максимальное количество составляет 100%. Проходной составляет 69%. Обучающийся, набравший более 69 -80% получает оценку «удовлетворительно», 81 – 95% оценку «хорошо», 96-100% оценку «отлично». Время на выполнение тестового задания – 60 минут.

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

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.

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	Темы собеседований, предусмотренные рабочей программой дисциплины, проводятся во время практических занятий. Преподаватель задает не менее двух вопросов по темам собеседований.. Во время выполнения собеседования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения собеседований, доводит до учащихся темы собеседований.
Реферат	Обучаемый самостоятельно или под руководством преподавателя выбирает тему, изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит реферат по результатам освоения темы, объемом до 15 стр. текста размером 12 пунктов, интервал 1,5; представляет сообщение/доклад преподавателю.
Сообщение, доклад	Обучаемый самостоятельно или под руководством преподавателя выбирает тему, изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит сообщение или доклад по результатам освоения темы, объемом до 20 стр. текста размером 12 пунктов, интервал 1,5; представляет сообщение/доклад преподавателю, отвечает на его вопросы.

Для организации и проведения промежуточной аттестации (в форме экзамена) 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 к зачету/экзамену для оценки знаний;

– перечень типовых простых практических заданий к зачету/экзамену для оценки умений;

– перечень типовых практических заданий к зачету/экзамену для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету/экзамену 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

При проведении промежуточной аттестации в форме экзамена могут быть использованы результаты тестирования:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	Обучающийся к экзамену допущен
Обучающийся набрал при тестировании менее 69 баллов	Обучающийся к экзамену не допущен

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам. Билеты составлены таким образом, что в 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; три практических задания: два из них для оценки умений (выбираются из перечня типовых простых практических заданий к экзамену); третье 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 ФОС на бумажном носителе в составе ФОС по дисциплине.

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.

Образец экзаменационного билета

<table>
<tr>
<td>ИРГУПС
2021-2022
учебный год</td>
<td>Экзаменационный билет № 1
по дисциплине «Информационная безопасность критической информационной инфраструктуры»

Профиль «Безопасность информационных систем и технологий»
7 семестр</td>
<td>Утверждаю:
И.о.аведующий кафедрой «ИСиЗИ» ИрГУПС
Т.К. Кириллова</td>
</tr>
<tr>
<td colspan="3">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.</td>
</tr>
</table>