ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «31» мая 2024 г. № 425-1

Б1.О.12 Защищенные информационные системы

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. – 8
Часов по учебному плану (УП) – 288

Формы промежуточной аттестации
очная форма обучения:
зачет 1 семестр, экзамен 2 семестр, курсовая работа 2 семестр

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

Семестр	1	2	**Итого**
Вид занятий	Часов по УП	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	68	85	**153**
– лекции	34	34	**68**
– практические (семинарские)	17		**17**
– лабораторные	17	51	**68**
Самостоятельная работа	40	59	**99**
Экзамен		36	**36**
Итого	108	180	**288**

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 «21» мая 2024 г. № 11

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 созданию и эксплуатации защищенных информационных систем, безопасных продуктов и систем информационных технологий, а также методов противодействия угрозам безопасности
1.2 Задачи дисциплины	
1	изучение методов оценки уровня защищенности информационных систем
2	освоение необходимых знаний по изучению методам противодействия угрозам безопасности
3	формирование умений и знаний по созданию и эксплуатации защищенных информационных систем
4	освоение методов организации и планирования мероприятий по обеспечению безопасности информационных систем
5	изучение методов оценки уровня защищенности информационных систем
6	освоение необходимых знаний по изучению методам противодействия угрозам безопасности
7	формирование умений и знаний по созданию и эксплуатации защищенных информационных систем

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть
2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины	
1	Б1.О.06 Моделирование технических объектов и систем управления
2	Б1.О.09 Теория систем и системный анализ
3	Б1.В.ДВ.01.01 Проектирование информационных систем
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.03 Лидерство и командообразование
2	Б2.О.03(П) Производственная - проектная практика
3	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
4	Б3.02(Д) Защита выпускной квалификационной работы

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Знает порядок проведения предпроектного обследования объектов информатизации, средства и особенности их защиты	Знать: порядок и требования к проведению предпроектного обследования объектов информатизации; понятие, виды и структуру автоматизированных систем; понятие и составляющие безопасности автоматизированных систем; схемы каталогизации угроз безопасности КС, способы их идентификации, спецификации и оценивая, роль человеческого фактора в угрозах безопасности ИС; понятия функциональной и системной архитектуры КС, ядра (монитора, системы) безопасности ИС
		Уметь: идентифицировать и оценивать угрозы безопасности при проведении предпроектного обследования ИС; определять и оформлять класс защищенности, проектируемой ИС
		Владеть: навыками работы с требованиями нормативно-правовых актов и нормативно- методических документов в сфере защиты информации при проведении предпроектного обследования объектов информатизации
	ОПК-1.2 Умеет оформить результаты предпроектного обследования объектов информатизации в виде требований на создание системы обеспечения ИБ	Знать: общую характеристику и методологию руководящих документов ФСТЭК по защите средств вычислительной техники (СВД) и автоматизированных систем (АС) от несанкционированного доступа к информации, классы защищенности и структуру функциональных требований к подсистемам защиты информации; общую характеристику и структуру стандартов по безопасности информационных технологий
		Уметь: составлять и правильно оформлять основные разделы Технического задания на проектирование несложных ИС

		(системы защиты информации ИС)
		Владеть: навыками проведении предпроектного обследования ИС на предмет проектирования систем защиты информации
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1 Участвует в формировании структуры (стадий и этапов) жизненного цикла изделия	Знать: методы управления проектами; этапы жизненного цикла проекта; модель жизненного цикла и порядок создания АС, стандарты и их содержание по регламентации стадий и этапов создания АС, структуру, порядок составления, оформления и утверждения
		Уметь: анализировать структуру, порядок составления, оформления и утверждения Технического задания по созданию АС, и изделий ИС, а также состав и структуру основных документов
		Владеть: навыками выбора наиболее эффективных методов управления проектами на этапах их жизненного цикла
	УК-2.2 Осуществляет эффективное управление проектом на всех этапах жизненного цикла для достижения конечного результата	Знать: состав и структуру основных документов; модель жизненного цикла и порядок создания изделий ИС, удовлетворяющих требованиям безопасности, способы задания требований безопасности, структуру, порядок разработки, оценки, утверждения и опубликования профилей защиты изделий ИТ, заданий по безопасности при создании ИС
		Уметь: анализировать: методы управления проектами; этапы жизненного цикла при. создания АС, стандарты и их содержание по регламентации стадий и этапов создания АС
		Владеть: навыками работы с нормативно-правовыми актами и нормативно- методическими документами в сфере защиты информации в ИС и внедрения их в практику на всех этапах жизненного цикла
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.2 Определяет приоритеты личностного роста и способы совершенствования собственной деятельности на основе самооценки и самообучения	Знать: свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания, а также возможности их самостоятельного, критического изучения и осмысления
		Уметь: определять приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям
		Владеть: способностью выстраивать гибкую профессиональную траекторию, используя инструменты непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда

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. Информационные системы.**						
1.1	Понятие, виды и структура информационных систем. Понятие защищенной ИС	1	4				ОПК-1.1 ОПК-1.2 УК-2.2
1.2	Основные понятия, категории и инструменты проектирования, разработки, внедрения и управления информационными технологиями предприятия и информационной защиты	1	4	2		14	ОПК-1.1 УК-2.2
1.3	Создание простой базы данных и разграничение доступа с помощью пароля. Оценка стойкости парольной защиты	1	4		10		ОПК-1.2 УК-6.2
2.0	**Раздел 2. Угрозы безопасности ИС.**						
2.1	Объекты защиты и угрозы безопасности в информационных системах	1	4				ОПК-1.1 УК-6.2
2.2	Виды угроз безопасности ИС, оценка угроз безопасности информации в ИС.	1	4	2		14	ОПК-1.2 УК-2.1
2.3	Идентификация и аутентификация средствами Dallas Lock.	1	4		10		ОПК-1.1 УК-6.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
3.0	**Раздел 3. Методы защиты ИС.**						
3.1	Методы защиты от основных видов угроз и перекрытие уязвимостей	1	4				ОПК-1.2 УК-2.2
3.2	Методика оценки угроз безопасности информации	1	4	4		13	ОПК-1.2 УК-2.1 УК-6.2
3.3	Контроль целостности программно-аппаратной среды и ресурсов файловой системы (Dallas Lock). к объектам ФС: локальным, глобальным, сетевым, аппаратным ресурсам, сменным накопителям. (Dallas Lock).	1	4		10		ОПК-1.2 УК-6.2
3.4	Разграничение доступа: (Дискреционный принцип, Мандатный принцип)	1			10		ОПК-1.2 УК-2.2 УК-6.2
	Форма промежуточной аттестации – зачет	1					ОПК-1.1 ОПК-1.2 УК-2.1 УК-6.2
4.0	**Раздел 4. Жизненный цикл ИС.**						
4.1	Жизненный цикл и порядок создания защищенных ИС	2	4				ОПК-1.1 УК-2.1 УК-2.2
4.2	Состав требований по защите информационных систем на этапах жизненного цикла.	2	2	3		14	ОПК-1.1 ОПК-1.2 УК-2.2
4.3	Международные и российские стандарты и другие НПА в области раз-работки программных средств	2	2		4		ОПК-1.1 УК-2.1
5.0	**Раздел 5. Методы проектирования защищенных ИС. Нормативно-правовая база.**						
5.1	Основы методов и технологий проектирования защищенных информационных систем.	2	4				ОПК-1.2 УК-2.2
5.2	Методы проектирования защищенных ИС. Нормативно-правовая база.	2	4	2		16	ОПК-1.1 УК-2.1
5.3	Аппаратные устройства и программные приложения для обеспечения ИБ	2	4		8		ОПК-1.2 УК-6.2
6.0	**Раздел 6. Эксплуатация защищенных ИС.**						
6.1	Администрирование и эксплуатация защищенных ИС	2	4				ОПК-1.1 ОПК-1.2 УК-2.2
6.2	Анализ среды предприятия с точки зрения информационной безопасности, выявление ключевых элементов и оценка их влияние на предприятие	2	2	2		12	ОПК-1.2 УК-2.1
6.3	Создание и анализ журналов (журнал входов, журнал управления учетными записями, журнал доступа к ресурсам, журнал печати, журнал управления политиками, журнал процессов) (Dal-las Lock)	2	2		10		ОПК-1.1 УК-2.2
7.0	**Раздел 7. Документальное оформление безопасности ИС.**						
7.1	Политика безопасности и основные требования к ее построению	2	2				ОПК-1.2 УК-2.1
7.2	Формирование основных разделов политики безопасности	2	2	2		16	ОПК-1.2 УК-6.2
7.3	Удаление файлов и зачистка остаточной информации: автоматически и по команде (Dallas Lock)	2			6		ОПК-1.2 УК-2.2
	Форма промежуточной аттестации – экзамен	2	36				ОПК-1.1 ОПК-1.2 УК-2.1 УК-2.2 УК-6.2
	Итого часов (без учёта часов на промежуточную аттестацию)		68	17	68	99	

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	Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 96 с. — URL: https://e.lanbook.com/book/167186 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Абденов, А. Ж. Анализ, описание и оценка функциональных узлов SIEM-системы : учебное пособие / А. Ж. Абденов, В. А. Трушин, К. Сулайман ; Новосибирский государственный технический университет. — Новосибирск : Новосибирский государственный технический университет, 2018. — 122 с. — URL: https://biblioclub.ru/index.php?page=book&id=576083 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.1.3	Корниенко, А. А. Риск-модели информационной безопасности : учебное пособие / А. А. Корниенко, С. В. Корниенко, А. П. Глухов, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2021. — 79 с. — URL: https://e.lanbook.com/book/191006 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.4	Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — URL: https://e.lanbook.com/book/180099 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Мошак, Н. Н. Основы управления информационной безопасностью : учебное пособие / Н. Н. Мошак. — Санкт-Петербург : ГУАП, 2022. — 141 с. — URL: https://e.lanbook.com/book/340967 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн

6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Серёдкин С.П. Методические указания по изучению дисциплины Б1.О.12 Защищенные информационные системы по направлению подготовки 10.04.01 Информационная безопасность, профиль Безопасность информационных систем и технологий /к.э.н. С.П. Серёдкин; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 14 с - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47498_1506_2024_1_signed.pdf	Онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»

6.2.1	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/
6.2.2	Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/

6.3 Программное обеспечение и информационные справочные системы

6.3.1 Базовое программное обеспечение

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

6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License
6.3.2 Специализированное программное обеспечение	
6.3.2.1	прогр.средство защиты от НСД Secret Net4.0, клиент серв.безоп.Secret Net 4.0, сервер безопасности С Secret Net4.0, система разгр.доступа Dallas Lock 7.0
6.3.2.2	MathCAD_student 15.0 Academic_License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01
6.3.2.3	Python 3.9, свободно распространяемое программное обеспечение https://docs.python.org/3/license.html
6.3.2.4	Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/
6.3.2.5	MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01.
6.3.2.6	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01.
6.3.3 Информационные справочные системы	
6.3.3.1	Не предусмотрены
6.4 Правовые и нормативные документы	
6.4.1	Не предусмотрены

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

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Лаборатория Д-523 «Моделирование и разработка программных систем и защита информации» для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной) Измеритель шумов и вибрации 003-МЗ
4	Лаборатория Д-523 «Моделирование и разработка программных систем и защита информации».«Безопасность программно-аппаратных средств защиты информации» для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор(переносной),экран(переносной),компьютер
5	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 «Защищенные информационные системы» 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	

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.12 Защищенные информационные системы

Приложение № 1 к рабочей программе

Специальность – 10.04.01 Информационная безопасность
Специализация – Безопасность информационных систем и технологий

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.12 Защищенные информационные системы прошел экспертизу на соответствие требованиям ФГОС по направлению 10.04.01 Безопасность информационных систем и технологий (уровень магистратуры), рассмотрен и рекомендован к внедрению на заседании СОП по специальности
«Информационная безопасность».

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

Б1. О.12 Защищенные информационные системы участвует в формировании компетенций:

ОПК-1 способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание; УК-2 способен управлять проектом на всех этапах его жизненного цикла; УК-6 способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.

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	Текущий контроль			
1.1	Текущий контроль	Создание простой базы данных и разграничение доступа с помощью пароля. Оценка стойкости парольной защиты	ОПК-3 УК-6	Лабораторная работа Защита лабораторной работы
1.2	Текущий контроль	Самостоятельное углубленное изучение лекционных материалов по теме «Угрозы безопасности ИС». Концепции информационной безопасности. Методы разработки общей и частных политик информационной безопасности.	ОПК-3 ОПК-1	Конспект (письменно). Компьютерные технологии Дискуссия на практических занятиях
2.0	Текущий контроль			
2.1	Промежуточная аттестация – зачёт	Разделы: 1.Информационные системы. 2.Угрозы безопасности ИС.		Собеседование (устно), комплект контрольных вопросов к зачету.
2.2		**2 семестр**		
2.3	Текущий контроль	Самостоятельное углубленное изучение лекционных материалов по теме «Методы защиты ИС». Работа в интернет. Анализ и построение защиты локальных внутренних и распределенных внешних вычислительных и ин-формационных сетей/Ср/	ОПК-3	Конспект (письменно). Компьютерные технологии Дискуссия на практических занятиях
2.4	Текущий контроль	Контроль целостности программно-аппаратной среды и ресурсов файловой системы (Dallas Lock). /Лаб	ОПК-3	Лабораторная работа Защита лабораторной работы
3.0	Текущий контроль			
3.1	Текущий контроль	Самостоятельное углубленное изучение лекционных материалов по теме «Жизненный цикл ИС». Работа в интернет. Международные и российские стандарты и другие НПА в области раз-работки программных средств /Ср/	ОПК-3	Конспект (письменно). Компьютерные технологии Дискуссия на практических занятиях
	Текущий контроль	Самостоятельное углубленное изучение лекционных материалов по теме «Методы проектирования защищенных ИС. Нормативно-правовая база». Работа в интернет. Аппаратные устройства и программные приложения для обеспечения ИБ/Ср/		Конспект (письменно). Компьютерные технологии Дискуссия на практических занятиях
	Текущий контроль	Самостоятельное углубленное изучение лекционных материалов по теме «Эксплуатация защищенных ИС». Работа в интернет.		Конспект (письменно). Компьютерные технологии Дискуссия на практических занятиях

		Анализ среды предприятия с точки зрения информационной безопасности, выявление ключевых элементов и оценка их влияние на предприятие. /Ср/		
	Текущий контроль	Разработка конкретных мер по обеспечению корпоративной информационной безопасности с учетом конкурентной ситуации. Методика экономического анализа для оценки совокупной стоимости систем защиты информации и стоимости их сопровождения. /Ср/		Конспект (письменно). Компьютерные технологии Дискуссия на практических занятиях
	Текущий контроль	Создание и анализ журналов (журнал входов, журнал управления учетными записями, журнал доступа к ресурсам,журнал печати, журнал управления политиками, журнал процессов) (Dal-las Lock). /Лаб//		Лабораторная работа Защита лабораторной работы
	Текущий контроль	Аудит защищенности информационной системы ИрГУПС(Сканнер-ВС). /Лаб//		Лабораторная работа Защита лабораторной работы
	Текущий контроль	Анализ сетевого трафика (в т.ч. в коммутируемых сетях, физически разделенных) (Сканнер-ВС). /Лаб//		Лабораторная работа Защита лабораторной работы

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,	Вопросы по

		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	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
4	Защита лабораторной работы	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Темы лабораторных работ и требования к их защите

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Зачет (дифференцированный зачет)	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 (билетов) к зачету
2	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
3	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	Высокий

	учебного материала. Ответил на все дополнительные вопросы	
«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. Основные сетевые угрозы информационным ресурсам;

2. Типичные сетевые атаки;
3. Механизмы реализации атак в сетях TCP/IP;
4. Состав компонентов комплексной системы обеспечения информационной безопасности;
5. Методы сканирования портов;
6. Модели доступа;
7. Основные показатели экономической эффективности средств защиты;
8. Защита от разрушающих программных воздействий;
9. Дефекты, ошибки в ИС. Поиск и их ликвидация;
10. Имеющиеся информационные риски;
11. Методы физической защиты объектов;
12. Программные закладки и борьба с ними;
13. Схемы шифрования с открытым ключом;
14. Схемы несимметричного шифрования
15. Задачи мониторинга и сопровождения ПО.
16. Межсетевые экраны

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 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:

1. Дискреционная модель доступа;
2. Мандатная модель доступа;
3. Основные спецификации безопасных ИС;
4. Основные принципы организационных мер защиты;
5. Основные принципы физических мер защиты ИС;
6. Основные программные меры защиты ИС;
7. Технические меры защиты ИС
8. Основные правила профессиональной этики аудитора;
9. Описание «оранжевой книги»;
10. Бизнес-цели ИС и их достижение;
11. Управление рисками ИБ. Примеры идентификации рисков;
12. Защита ИС от несанкционированного использования;
13. Тестирование ИС на предмет ИБ;
14. Экономика защиты информации.

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

3.1.3 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.Понятие угрозы информации в современных системах ее обработки. Системная классификация угроз. Система показателей уязвимости информации. Методы и модели оценки уязвимости информации;

2.Криптографические протоколы и основные требования к ним; протоколы “рукопожатия”; протоколы установления подлинности; протоколы идентификации и аутентификации;

3.Большие простые и псевдопростые числа. Их применение в криптографии (в каких криптографических системах);

4.Криптография с открытым ключом. Предпосылки появления. Однонаправленные функции с секретом и их применения. Схемы шифрования с открытым ключом и цифровой подписи. Основные принципы;

5.Основы защиты информации от утечки по техническим каналам и физическая защита;

6.Методы и средства инженерной защиты и технической охраны объектов; скрытие объектов наблюдения;

7.Скрытие речевой информации в каналах связи; энергетическое скрытие акустических информативных сигналов; обнаружение и локализация закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей;

8.Экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов:

9.Средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа;

10.Основные методы и средства защиты информации от утечки по техническим каналам;

11.Основные методы и средства защиты информации в каналах связи;

12.Защита от разрушающих программных воздействий, защита программ от изменения и контроль целостности, построение изолированной программной среды;

13.Организация управления доступом и защиты ресурсов ОС; основные механизмы безопасности: средства и методы аутентификации в ОС;

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 Типовые контрольные задания для проведения тестирования

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

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-1.1 ОПК-1.2 УК-2.2	Понятие, виды и структура информационных систем. Понятие защищенной ИС	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.1 УК-2.2	Основные понятия, категории и инструменты проектирования, разработки, внедрения и управления информационными технологиями предприятия и информационной защиты	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.2 УК-6.2	Создание простой базы данных и разграничение доступа с помощью пароля. Оценка стойкости парольной защиты	Знание	4 – ОТЗ 6 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
ОПК-1.1 УК-6.2	Объекты защиты и угрозы безопасности в информационных системах	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.2 УК-2.1	Виды угроз безопасности ИС, оценка угроз безопасности информации в ИС.	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.1 УК-6.2	Идентификация и аутентификация средствами Dallas Lock.	Знание	4 – ОТЗ 6 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
ОПК-1.2 УК-2.2	Методы защиты от основных видов угроз и перекрытие уязвимостей	Знание	4 – ОТЗ 6 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-1.2 УК-2.1 УК-6.2	Методика оценки угроз безопасности информации	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.2 УК-6.2	Контроль целостности программно-аппаратной среды и ресурсов файловой системы (Dallas Lock). к объектам ФС: локальным, глобальным, сетевым, аппаратным ресурсам, сменным накопителям. (Dallas Lock).	Знание	4 – ОТЗ 6 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ

ОПК-1.2 УК-2.2 УК-6.2	Разграничение доступа: (Дискреционный принцип, Мандатный принцип)	Знание	4 – ОТЗ 6 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
ОПК-1.1 УК-2.1 УК-2.2	Жизненный цикл и порядок создания защищенных ИС	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.1 ОПК-1.2 УК-2.2	Состав требований по защите информационных систем на этапах жизненного цикла.	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.1 УК-2.1	Международные и российские стандарты и другие НПА в области разработки программных средств	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.2 УК-2.2	Основы методов и технологий проектирования защищенных информационных систем.	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.1 УК-2.1	Методы проектирования защищенных ИС. Нормативно-правовая база.	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.2 УК-6.2	Аппаратные устройства и программные приложения для обеспечения ИБ	Знание	4 – ОТЗ 6 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
ОПК-1.1 ОПК-1.2 УК-2.2	Администрирование и эксплуатация защищенных ИС	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.2 УК-2.1	Анализ среды предприятия с точки зрения информационной безопасности, выявление ключевых элементов и оценка их влияние на предприятие	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.1 УК-2.2	Создание и анализ журналов (журнал входов, журнал управления учетными записями, журнал доступа к ресурсам, журнал печати, журнал управления политиками, журнал процессов) (Dal-las Lock)	Знание	4 – ОТЗ 6 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
ОПК-1.2 УК-2.1	Политика безопасности и основные требования к ее построению	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.2 УК-6.2	Формирование основных разделов политики безопасности	Знание	4 – ОТЗ 6 – ЗТЗ
ОПК-1.2 УК-2.2	Удаление файлов и зачистка остаточной информации: автоматически и по команде (Dallas Lock)	Знание	4 – ОТЗ 6 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык	2 – ОТЗ 2 – ЗТЗ
		Итого	144

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.

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-1.1 ОПК-1.3 ОПК-3.2	Тема 1. Понятие и задачи программной инженерии	Знание	5 – ОТЗ 5 – ЗТЗ
ОПК-1.2 ОПК-3.2	Тема 2. Проектирование программного обеспечения	Знание	4 – ОТЗ 6 – ЗТЗ

		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-1.2 ОПК-3.1 ОПК-3.2 ОПК-3.3	Тема 3. Жизненный цикл ПО от технического задания на разработку до завершения эксплуатации	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-3.1 ОПК-3.2	Тема 4. Стандарты и профили стандартов	Знание	4 – ОТЗ 4 – ЗТЗ
ОПК-1.1 ОПК-1.2	Тема 5. Системное проектирование приложений	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	4 – ОТЗ 4 – ЗТЗ
ОПК-1.1 ОПК-3.2	Тема 6. Обоснование разработки ПО	Знание	6 – ОТЗ 6 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 2 – ЗТЗ
ОПК-3.1	Тема 7. Модели жизненного цикла и их особенности	Знание	4 – ОТЗ 4– ЗТЗ
ОПК-1.1 ОПК-1.3	Тема 8. Применение визуального языка моделирования	Знание	4 – ОТЗ 4 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
ОПК-1.2 ОПК-3.2	Тема 9. Ресурсы ПО и управление ими	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-1.2 ОПК-3.2	Тема 10. Риски разработки ПО. Отладка ПО	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-1.1 ОПК-1.2	Тема 11. Верификация программных кодов	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-3.2	Тема 12. Сопровождение и мониторинг ПО	Знание	2 – ОТЗ 2 – ЗТЗ
ОПК-3.2 ОПК-3.3	Тема 13. Документирование ПО	Знание	2 – ОТЗ 2 – ЗТЗ
		Итого	120

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. 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.

2. Оценка рисков ИБ, включающая в себя:

А) Идентификацию риска ИБ и анализ риска ИБ;

Б) Идентификацию риска ИБ, анализ риска ИБ, сравнительную оценку риска ИБ; оценку остаточного риска;

В) Идентификацию риска ИБ, анализ риска ИБ, оценку остаточного риска, расчет ущерба.

3. Обработка рисков ИБ

А) Снижение, перенос, уклонение, принятие;

Б) Страхование;

В) Хеджирование.

4. 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).

5. Каким методами определяется уровень риска информационного актива:

А) Метод ожидаемых потерь;

Б) Затратный метод;

В) Метод аналогий.

6. Технические каналы утечки информации возникают:

А) При использовании злоумышленником специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию при непосредственном контакте с персоналом фирмы, документами, делами и базами данных;

Б) При использовании злоумышленником специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию без непосредственного контакта с персоналом фирмы, документами, делами и базами данных;

В) При использовании злоумышленником специальных технических средств для воздействия на средства защиты информации;

7. Основными техническими каналами являются:

А) Визуально-оптический;

Б) Акустический;

В) Электромагнитный.

8. Требования к защите информационных активов хозяйствующего субъекта- система защиты информационных активов;

   А) Должна быть представлена целостностью системы, должна обеспечивать безопасность информационных активов, средств обработки информации и защиту интересов участников информационных отношений, методы и средства защиты должны быть по возможности «прозрачными» для законного пользователя;

   Б) Должна обеспечивать информационные связи внутри системы между ее элементами для согласованного их функционирования и связи с внешней средой;

   В) Должна соответствовать требованиям принципа экономической целесообразности.

9. Категории информационных рисков:

   А) Риски, вызванные утратой и/или утечкой информации и использованием ее конкурентами или сотрудниками в целях, которые могут повредить бизнесу;

   Б) Риски технических сбоев работы каналов передачи информации, которые могут привести к убыткам;

   В) Риски, вызванные форс-мажорными обстоятельствами.

10. Угрозы безопасности информационным активам это:

    А) Совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации;

    Б) Совокупность условий и факторов, которые могут причинить ущерб информации;

    В) Совокупность условий и факторов, которые могут стать причиной нарушения информации.

11. Риск рассматривается, как поддающаяся измерению вероятность:

    А) Причинить негативные последствия;

    Б) Создать условия для наступления негативных последствий;

    В) Понести убытки или упустить выгоду.

12. Риск определяется:

    А) Вероятностью причинения ущерба и величиной ущерба, наносимого экономической системе или субъекту хозяйствования в случае осуществления угрозы безопасности информационным ресурсам;

    Б) Возможностью реализации угрозы информационной безопасности;

    В) Величиной ущерба.

13. Оценка рисков – это:

    А) Выбор параметров для их описания и получение оценок по этим параметрам;

    Б) Процедура выявления факторов рисков и оценки их значимости;

    В) Выявление характера последствий.

14. Стратегии управления различными классами информационных рисков:

А) Уклонение от риска, изменение характера риска, уменьшение степени риска;

Б) Принятие риска;

В) Уклонение от риска, изменение характера риска, уменьшение степени риска, принятие риска.

15. Целью анализа рисков является:

А) Оценка угроз и уязвимостей, возможного ущерба, учитывая уровень защищенности информационной системы;

Б) Проверка уровня защищенности информационной системы;

В) Оценка текущего состояния защищенности информационной системы.

16.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.

17. Системы безопасности должны обеспечивать:

а). восстановление функционирования системы безопасности информационной инфраструктуры;

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

в). устойчивое функционирование системы безопасности информационной инфраструктуры.

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).

3.1.4 Перечень теоретических вопросов к экзамену

1.Понятие национальной безопасности; виды безопасности; информационная безопасность (ИБ) в системе национальной безопасности Российской Федерации;
2.Общеметодологические принципы теории ИБ, анализ угроз ИБ;
3.Классификация угроз конфиденциальности, целостности и доступности информации; классификация каналов утечки и искажения информации;
4.Классификация методов и средств обеспечения ИБ;
5.Классификация угроз конфиденциальности, целостности и доступности информации; классификация каналов утечки и искажения информации;
6.Модели безопасности;
7.Политика безопасности;

8.Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем;
9.Построение парольных систем их применение к системам разграничения доступа, примеры практической реализации;
10.Криптография. Особенности реализации систем с симметричными и несимметричными ключами;
11.Методология обследования и проектирования систем защиты;
12.Понятие угрозы информации в современных системах ее обработки. Системная классификация угроз. Система показателей уязвимости информации. Методы и модели оценки уязвимости информации;
13.Криптографические протоколы и основные требования к ним; протоколы “рукопожатия”; протоколы установления подлинности; протоколы идентификации и аутентификации;
14.Большие простые и псевдопростые числа. Их применение в криптографии (в каких криптографических системах);
15.Криптография с открытым ключом. Предпосылки появления. Однонаправленные функции с секретом и их применения. Схемы шифрования с открытым ключом и цифровой подписи. Основные принципы;
16.Основы защиты информации от утечки по техническим каналам и физическая защита;
17.Методы и средства инженерной защиты и технической охраны объектов; скрытие объектов наблюдения;
18.Скрытие речевой информации в каналах связи; энергетическое скрытие акустических информативных сигналов; обнаружение и локализация закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей;
19.Экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов:
20.Средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа;
21.Основные методы и средства защиты информации от утечки по техническим каналам;
22.Основные методы и средства защиты информации в каналах связи;
23.Защита от разрушающих программных воздействий, защита программ от изменения и контроль целостности, построение изолированной программной среды;
24.Организация управления доступом и защиты ресурсов ОС; основные механизмы безопасности: средства и методы аутентификации в ОС;
25.Основные положения критериев TCSEC («Оранжевая книга» США). Фундаментальные требования компьютерной безопасности. Требования классов защищенности;
26.Основные положения Руководящих документов Гостехкомиссии России в области защиты информации. Определение и классификация нарушителя. Классы защищенности АС от НСД к информации;
27.Основные положения CCITCE («Единые критерии» Европы). Структура профиля и проекта защиты. Структура и ранжирование функциональных требований. Требования доверия;
28.Средства обеспечения безопасности баз данных: средства идентификации и аутентификации объектов баз данных, языковые средства разграничения доступа, концепция и реализация механизма ролей;
29.Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ);
30.Жизненный цикл автоматизированной системы; этапы проектирования системы; организация работ, функции заказчиков и разработчиков;
31.Методы сканирования портов;
32.Методы обнаружения пакетных сниферов;
33. Методы перехвата сетевых соединений в сетях TCP/IP;
34.Атаки, направленные на маршрутизаторы;
35.Несанкционированный обмен данными;
36.Примеры типичных сетевых атак;
37.Виртуальные частные сети (VPN);

38.Протокол IPSEC;
39.Сетевые атаки. Стадии проведения сетевой атаки.Технические меры защиты от сетевых атак;
40.Классификации сетевых угроз, уязвимостей и атак;
41.Механизмы реализации атак в сетях TCP/IP;
42.Характеристика моделей доступа;
43.Внутренний аудит ИС. Его задачи;
44.Внешний аудит ИС. Его задачи;
45.Межсетевые экраны (МЭ)Основные возможности и схемы развертывания МЭ;
46.Построение правил фильтрации;
47. Методы сетевой трансляции адресов (NAT);
48. Методы обхода межсетевых экранов;
49.Системы обнаружения вторжений (СОВ);
50.Средства обнаружения уязвимостей сетевых служб;
51.Способы противодействия вторжениям;
52.Системы виртуальных ловушек (Honey Pot и Padded Cell);
53.Формирование и анализ модели нарушителя;
54.Организационные и правовые методы;
55.Методы борьбы с компьютерными вирусами;
56.Методы предотвращения шпионажа и диверсии;
57.Законодательство, затрагивающее аспекты и механизмы обеспечения безопасности (авторское право, защита персональных данных и т.д.);
58.Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001.

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/практики.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
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.
Защита лабораторной работы	Обучаемый выполняет работу самостоятельно или по указаниям преподавателя, готовит отчет по ЛР, отвечает на вопросы преподавателя. Оценка зачтено/незачтено ставится по результатам защиты ЛР. Если работа связана с разработкой или использованием программно-инструментальных средств, необходимо продемонстрировать владение этим средством и/или полученный с его помощью результат.

Для организации и проведения промежуточной аттестации (в форме зачета/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 зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Оценка
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация в форме зачета проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач (не более двух теоретических и двух практических). Промежуточная аттестация в форме зачета с проведением аттестационного испытания в форме собеседования проходит на последнем занятии по дисциплине.

Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения

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

2021-2022 учебный год	**Экзаменационный билет № 1** **по дисциплине «Защищенные информационные системы»** **Специализация/профиль** «Безопасность информационных систем и технологий» 3 **семестр**	Утверждаю: Заведующий кафедрой «ИСиЗИ» ИрГУПС Т.К. Кириллова

1.Оценка возможных последствий реализации угроз безопасности информации.

2.Реагирование на компьютерные инциденты в ходе эксплуатации ИС.

3.Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности ИС.

Варианты размеров билета:
Билет формата А5 – 148*210мм
Билет формата А4 – 210*297мм