ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

Б1.О.49 Методология анализа информационных рисков

рабочая программа дисциплины

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

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

Формы промежуточной аттестации
очная форма обучения:
экзамен 8 семестр

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

Семестр	8	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	68	**68**
– лекции	34	**34**
– практические (семинарские)	34	**34**
– лабораторные		
Самостоятельная работа	40	**40**
Экзамен	36	**36**
Итого	144	**144**

ИРКУТСК

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

Программу составил(и):

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «30» ноября 20-1 г. №

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

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели дисциплины

1	раскрытие сущности и значения методологии анализа информационных рисков реализации угроз, как основы информационной безопасности и защиты информации;
2	определение теоретических, концептуальных, методических и организационных основ информационной безопасности и защиты ценной для предприятия информации

1.2 Задачи дисциплины

1	изучить понятие «информационных активов» как основной характеристики системы оценки информационных рисков хозяйствующего субъекта;
2	определить место, роль, специфику системы оценки информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия;
3	оценить существующие методические подходы к оценке информационных рисков для выявления возможностей совершенствования данной деятельности;
4	изучить особенности организационного направления в деятельности по защите информационных активов и определение их влияния на создание и развитие системы защиты информационных активов хозяйствующего субъекта;
5	освоить методические положения по совершенствованию деятельности в сфере оценки информационных рисков хозяйствующих субъектов;
6	освоить методические подходы к оценке эффективности деятельности по защите информационных активов предприятия

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.
Цель достигается по мере решения в единстве следующих задач:
– формирование сознательного отношения к выбранной профессии;
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;
– формирование психологии профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть

2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины

1	Дисциплина изучается на начальном этапе формирования компетенции

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

1	Б1.О.44 Информационная безопасность открытых систем
2	Б1.О.46 Аудит информационных технологий и систем обеспечения информационной безопасности
3	Б1.О.60 Защита информации от несанкционированного доступа
4	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
5	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-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных	ОПК-13.1 Знает основы диагностики и тестирования систем защиты информации автоматизированных систем	Знать: роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия; основные виды информационных активов (ресурсов) хозяйствующего субъекта
		Уметь: определять состав, важность и ценность

систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем		конфиденциальной информации применительно к видам тайны; выявлять информационные риски реализации угроз информационным активам предприятия и иным объектам защиты
		Владеть: основными методами выявления информационных рисков реализации угроз конфиденциальной информации; методами определения уровня информационных рисков
	ОПК-13.2 Умеет проводить анализ защищенности, в том числе выявлять и оценивать опасность уязвимостей систем защиты информации и угроз информационной безопасности автоматизированных систем	Знать: основные виды угроз информационной безопасности хозяйствующего субъекта и уязвимости ресурсов, через которые они могут быть реализованы; особенности и проблемы организационного направления в деятельности по защите информационных активов
		Уметь: разрабатывать модели угроз и нарушителя информационной безопасности предприятия; определять направления и виды защиты информации с учетом характера рисков реализации угроз информационным активам предприятия
		Владеть: методами оценки возврата инвестиций от реализации контрмер по защите информации, и их эффективности; навыками работы со специальными программными комплексами управления информационными рисками предприятия
	ОПК-13.3 Имеет базовые навыки проведения диагностики и тестирования систем защиты информации автоматизированных систем	Знать: методический подход к оценке защищенности информационных активов хозяйствующего субъекта на основе учета информационных рисков; основные направления по применению защитных мероприятий с целью увеличения рискозащищенности информационных активов предприятия
		Уметь: выявлять недостатки (уязвимости) в функционировании системы защиты информации автоматизированной системы
		Владеть: терминологией и системным подходом к выявлению недостатков (уязвимостей) информационных систем (АС); навыками анализа угроз ИБ и уязвимостей в АС; организационными, организационно-техническими, техническими и компьютерными средствами по контролю защиты информации в АС
ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1 Знает основные методы инструментального мониторинга и аудита защищенности автоматизированных систем	Знать: существующие методические подходы к оценке информационных рисков и основные тенденции развития систем информационной рискозащищенности хозяйствующих субъектов
		Уметь: анализировать и оценивать угрозы безопасности при формировании требований пользователя к АС
		Владеть: методологией анализа информационных рисков
	ОПК-15.2 Умеет администрировать средства и системы защиты информации автоматизированных систем	Знать: механизмы оценки последствия от реализации угроз безопасности
		Уметь: проводить анализ оценки угроз безопасности информации, с целью повышения эффективности средств и методов ЗИ в АС
		Владеть: методикой оценки угроз ИБ
	ОПК-15.3 Имеет базовые навыки контроля функционирования средств и систем управления информационной	Знать: руководящие документы, по оценке угроз безопасности информации
		Уметь: анализировать угрозы ИБ
		Владеть: способностью оценивать последствия от реализации угроз безопасности информации в

	безопасностью автоматизированных систем	автоматизированной системе

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. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия.**						
2.0	**Раздел 2. Основные этапы и элементы управления рисками и их оценки.**						
3.0	**Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.**						
4.0	**Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.**						
	Итого часов (без учёта часов на промежуточную аттестацию)		34	34		40	

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ 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.49 Методология анализа информационных рисков по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация – Безопасность открытых информационных систем / С.П. Серёдкин ; ИрГУПС. – Иркутск : ИрГУПС, 2021. – 12 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_9164_1529_2021_1_signed.pdf	Онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»

6.3 Программное обеспечение и информационные справочные системы

6.3.1 Базовое программное обеспечение

6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные

	приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License
6.3.2 Специализированное программное обеспечение	
6.3.2.1	Не предусмотрено
6.3.3 Информационные справочные системы	
6.3.3.1	Не предусмотрены
6.4 Правовые и нормативные документы	
6.4.1	Не предусмотрены

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

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-216 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
4	Учебная аудитория Д-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
5	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма

занятие	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 «Методология анализа информационных рисков» 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	

ИРКУТСК
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «___» _____ 20__ г. № ___

Б1.О.49 Методология анализа информационных рисков
рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – специализация N 5 "Безопасность открытых информационных систем"
Квалификация выпускника – Специалист по защите информации

Форма и срок обучения – 5л 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 - 8.

Общая трудоемкость в з.е. – 4
Часов по учебному плану (УП) – 144 Формы промежуточной аттестации в семестрах
Экзамен-8.

Распределение часов дисциплины по семестрам

Семестр	8	**Итого**
Число недель в семестре	16	
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в форме ПП*	**68/4**	**68/4**
– лекции	34	34
– практические (семинарские)	34/4	34/4
– лабораторные	-	-
Самостоятельная работа	**40**	**40**
Экзамен	**36**	**36**
Итого	**144**	**144**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – направление подготовки 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 заведующей кафедрой «ИСиЗИ» Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели дисциплины	
1	- раскрытие сущности и значения методологии анализа информационных рисков реализации угроз, как основы информационной безопасности и защиты информации, определение теоретических, концептуальных, методических и организационных основ информационной безопасности и защиты ценной для предприятия информации.
1.2 Задачи дисциплины	
1	– изучить понятие «информационных активов» как основной характеристики системы оценки информационных рисков хозяйствующего субъекта.
2	– определить место, роль, специфику системы оценки информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия.
3	– оценить существующие методические подходы к оценке информационных рисков для выявления возможностей совершенствования данной деятельности.
4	– изучить особенности организационного направления в деятельности по защите информационных активов и определение их влияния на создание и развитие системы защиты информационных активов хозяйствующего субъекта.
5	– освоить методические положения по совершенствованию деятельности в сфере оценки информационных рисков хозяйствующих субъектов.
6	– освоить методические подходы к оценке эффективности деятельности по защите информационных активов предприятия.
	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: Методы и средства криптографической защиты информации Защита объектов критической информационной инфраструктуры. Производственная - проектно-технологическая	
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Моделирование процессов и систем защиты информации
2	Проектирования систем защиты объектов информатизации
3	Производственная практика - преддипломная

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Код и наименование	**Код и наименование**	**Планируемые результаты обучения**

компетенции	индикатора достижения компетенции	
ОПК-13Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем.	ОПК-13.1Знает основы диагностики и тестирования систем защиты информации автоматизированных систем. ОПК-13.2Умеет проводить анализ защищенности, в том числе выявлять и оценивать опасность уязвимостей систем защиты информации и угроз информационной безопасности автоматизированных систем. ОПК-13.3Имеет базовые навыки проведения диагностики и тестирования систем защиты информации автоматизированных систем.	**Знать:** Роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия; Основные виды информационных активов (ресурсов) хозяйствующего субъекта; Основные виды угроз информационной безопасности хозяйствующего субъекта и уязвимости ресурсов, через которые они могут быть реализованы; Особенности и проблемы организационного направления в деятельности по защите информационных активов; Методический подход к оценке защищенности информационных активов хозяйствующего субъекта на основе учета информационных рисков; Основные направления по применению защитных мероприятий с целью увеличения рискозащищенности информационных активов предприятия. **Уметь:** Определять состав, важность и ценность конфиденциальной информации применительно к видам тайны; Выявлять информационные риски реализации угроз информационным активам предприятия и иным объектам защиты; Разрабатывать модели угроз и нарушителя информационной безопасности предприятия; Определять направления и виды защиты информации с учетом характера рисков реализации угроз информационным активам предприятия; Выявлять недостатки (уязвимости) в функционировании системы защиты информации автоматизированной системы; **Владеть:** Основными методами выявления информационных рисков реализации угроз конфиденциальной информации; Методами определения уровня информационных рисков; Методами оценки возврата инвестиций от реализации контрмер по защите информации, и их эффективности; Навыками работы со специальными программными комплексами

		управления информационными рисками предприятия; Терминологией и системным подходом к выявлению недостатков (уязвимостей) информационных систем (АС); Навыками анализа угроз ИБ и уязвимостей в АС; Организационными, организационно-техническими, техническими и компьютерными средствами по контролю защиты информации в АС ..
ОПК-15Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;	ОПК-15.1Знает основные методы инструментального мониторинга и аудита защищенности автоматизированных систем. ОПК-15.2Умеет администрировать средства и системы защиты информации автоматизированных систем. ОПК-15.3 Имеет базовые навыки контроля функционирования средств и систем управления информационной безопасностью автоматизированных систем	**Знать:** Существующие методические подходы к оценке информационных рисков и основные тенденции развития систем информационной рискозащищенности хозяйствующих субъектов; Механизмы оценки последствия от реализации угроз безопасности. Руководящие документы, по оценке угроз безопасности информации**.** **Уметь:** Анализировать и оценивать угрозы безопасности при формировании требований пользователя к АС; Проводить анализ оценки угроз безопасности информации, с целью повышения эффективности средств и методов ЗИ в АС. **Владеть:** Методологией анализа информационных рисков; Методикой оценки угроз ИБ. Выявлять уязвимости в основных компонентах АС и разрабатывать мероприятия по их устранению. Способностью оценивать последствия от реализации угроз безопасности информации в автоматизированной системе.

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. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия.**	8					
1.1	Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления. /Лек/		4				ОПК-13.1 ОПК-13.2 ОПК-13.3
1.2	Идентификация активов (описание бизнес-процессов). /Пр/			1			ОПК-15.1 ОПК-15.2 ОПК-15.3

1.3	Термины и определения области управления информационными рисками. /Ср/					6	ОПК-13.2 ОПК-13.3
1.4	Антология кибератак. Наихудшие сценарии кибератак. /Ср/						ОПК-13.2 ОПК-13.3
2.0	**Раздел 2. Основные этапы и элементы управления рисками и их оценки.**	8					
2.1	Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками. /Лек/		4				ОПК-13.2 ОПК-13.3 ОПК-15.3
2.2	Определение ценности активов (критерии оценки ущерба, таблица ценности активов). /Пр/			1			ОПК-15.1 ОПК-15.2
2.3	Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности. /Лек/		4				ОПК-13.2 ОПК-13.3 ОПК-15.3
2.4	Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы. /Пр/			2			ОПК-15.1 ОПК-15.2
2.5	Базовый опросник для определения степени критичности систем по методу CRAMM. Опросный лист для оценки угроз по методу CRAMM. Опросный лист для оценки уязвимостей по методу CRAMM. /Ср/					4	ОПК-13.2 ОПК-13.3
2.6	Системный подход к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками, деятельности по управлению рисками (сопровождение и мониторинг механизмов безопасности, пересмотр и переоценка риска, управление документами и записями, корректирующие и превентивные меры, коммуникация рисков). Аутсорсинг процессов управления рисками. распределение ответственности за управление рисками. /Лек/						ОПК-13.2 ОПК-13.3 ОПК-15.3
2.7	Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков. /Пр/			1			ОПК-15.1 ОПК-15.2
2.8	Обработка рисков информационной безопасности. Процесс обработки рисков. Способы обработки риска (принятие, уменьшение, передача, избежание риска). Оценка возврата инвестиций в информационную безопасность. План обработки рисков. /Лек/		4				ОПК-13.2 ОПК-13.3 ОПК-15.3
2.9	Задание контрмер. Расчет риска реализации по всем угрозам для информационной системы после задания контрмер. Эффективность контрмеры. Эффективность комплекса контрмер. Расчет совокупной стоимости владения. Расчет возврата инвестиций. /Пр/			1	4		ОПК-15.1 ОПК-15.2
2.10	Декларация о применимости механизмов контроля. /Ср/					4	ОПК-13.2 ОПК-13.3
3.0	**Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.**	8					

3.1	Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками. /Лек/		4				ОПК-13.2 ОПК-13.3 ОПК-15.3
3.2	Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы. /Пр/			2			ОПК-15.1 ОПК-15.2
3.3	Программные продукты для управления рисками информационной безопасности. /Ср/					2	ОПК-13.2 ОПК-13.3
3.4	Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия. /Лек/		2				ОПК-13.2 ОПК-13.3 ОПК-15.3
3.5	Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001. /Пр/			2			ОПК-15.1 ОПК-15.2
3.6	Законодательные и нормативные акты Российской Федерации в области защиты информации. /Ср/					2	ОПК-13.2 ОПК-13.3
3.7	Изучение документов ГТК (защита от несанкционированного доступа к информации). /Ср/			2		4	ОПК-13.2 ОПК-13.3
3.8	BS ISO/IEC27001:2005 (BS 7799-2:2005). Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 779993:2006 ИISO/IEC 27005:2008 /Ср/					4	ОПК-13.2 ОПК-13.3
4.0	**Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.**	8					
4.1	Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности. /Лек/		2		4		ОПК-13.2 ОПК-13.3 ОПК-15.3
4.2	Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность. /Пр/			2			ОПК-15.1 ОПК-15.2
4.3	Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта. /Лек/		4				ОПК-13.2 ОПК-13.3 ОПК-15.3

4.4	Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта. /Пр/						ОПК-15.1 ОПК-15.2
4.5	Проработка лекционного материала. Подготовка к промежуточному тестированию. /Ср/					4	ОПК-13.2 ОПК-13.3
5.0	**Экзамен**	8					

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
Л1.1	Никитин И.А., Цулая М.Т.	Процессы анализа и управления рисками в области ИТ : учебное пособие. - 2-е изд. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=429089	М. : ИНТУИТ, 2016.	100 % онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке /100% онлайн
Л2.1	Аверченков В.И.	Аудит информационной безопасности : учебное пособие для вузов. - 2-е изд. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=93245	М. : Флинта, 2011.	100 % онлайн
Л2.2	Анисимов А.А.	Менеджмент в сфере информационной безопасности : курс лекций. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=232981	М. : Интернет-Университет ИТ, 2009	100 % онлайн
Л2.3	Нестеров С.А.	Анализ и управление рисками в информационных системах на базе операционных систем : учебное пособие. [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=234529	М. : Интернет-Университет ИТ, 2009.	100 % онлайн

6.1.3 Методические разработки

	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет	Кол-во экз. в библиотеке /100%

			обучающегося	онлайн
Л3.1	Н.И. Глухов	Оценка информационных рисков предприятия, учебное пособие.	Иркутск: ИрГУПС, 2013.	67
6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке /100% онлайн
Л4.1	Астахов А.М.	Искусство управления информационными рисками : учебное пособие.	М.: ДМК Пресс, 2010. / Личный кабинет	100% онлайн
Л4.2	Краковский Ю.М.	Методика определения информационных рисков	Личный кабинет	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	Федеральный закон от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о

	защите информации».
6.4.2	Федеральный закон от 26 июня 2017г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6.4.3	Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 30.12.2020) "О персональных данных"
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	Нормативно-правовые акты государственных, муниципальных органов, предприятий в области информационной безопасности

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.49 Методология анализа информационных рисков
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.49 «Методология анализа информационных рисков» 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

Б1.О.49 Методология анализа информационных рисков участвует в формировании компетенций:

ОПК-13.1Знает основы диагностики и тестирования систем защиты информации автоматизированных систем;

ОПК-13.2Умеет проводить анализ защищенности, в том числе выявлять и оценивать опасность уязвимостей систем защиты информации и угроз информационной безопасности автоматизированных систем;

ОПК-13.3Имеет базовые навыки проведения диагностики и тестирования систем защиты информации автоматизированных систем;

ОПК-15.1Знает основные методы инструментального мониторинга и аудита защищенности автоматизированных систем;

ОПК-15.2Умеет администрировать средства и системы защиты информации автоматизированных систем;

ОПК-15.3 Имеет базовые навыки контроля функционирования средств и систем управления информационной безопасностью автоматизированных систем.

Программа контрольно-оценочных мероприятий очная форма обучения

№	Недел я	Наименование контрольно-оценочного мероприятия	Объект контроля (понятие/тем/раздел и т.д. дисциплины)	Код индикатор а достижени я компетенци и	Наименование оценочного средства (форма проведения*)
1.			**Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия.**		
2.	1.	Текущий контроль	Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления. /Лек/	ОПК-13.1 ОПК-13.2 ОПК-15.3	Конспект (письменно). Компьютерные технологии
3.	1	Текущий контроль	Идентификация активов (описание бизнес-процессов). /Пр/	ОПК-15.2 ОПК-15.3 ОПК-13.1	Конспект (письменно). Дискуссия на практических занятиях
4.	2	Текущий контроль	Термины и определенияв области управления информационнымирисками. /Ср/	ОПК-13.1 ОПК-13.2 ОПК-15.1 ОПК-15.2	Конспект (письменно). Компьютерные технологии
5.	2	Текущий контроль	Антология кибератак. Наихудшие сценарии кибератак. /Ср/	ОПК-13.1 ОПК-13.2 ОПК-15.1 ОПК-15.2	Конспект (письменно). Компьютерные технологии
6			**Раздел 2. Основные этапы и элементы управления рисками и их оценки.**		
7	3	Текущий контроль	Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками.	ОПК-13.1 ОПК-13.2 ОПК-15.3	Конспект (письменно). Компьютерные технологии

			/Лек/		
8	3	Текущий контроль	Определение ценности активов (критерии оценки ущерба, таблица ценности активов). /Пр/	ОПК-15.2 ОПК-15.3 ОПК-13.1	Конспект (письменно). Дискуссия на практических занятиях
9	4	Текущий контроль	Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности. /Лек/	ОПК-13.1 ОПК-13.2 ОПК-15.3	Конспект (письменно). Компьютерные технологии
10	4	Текущий контроль	Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы. /Пр/	ОПК-15.2 ОПК-15.3 ОПК-13.1	Конспект (письменно). Дискуссия на практических занятиях
11	4	Текущий контроль	Базовый опросникдля определения степени критичности системпо методу CRAMM. Опросный лист для оценки угроз по методу CRAMM. Опросный лист для оценкиуязвимостей по методу CRAMM. /Ср/	ОПК-13.1 ОПК-13.2 ОПК-15.1 ОПК-15.2	Конспект (письменно). Компьютерные технологии
12	5	Текущий контроль	Системный подход к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками, деятельности по управлению рисками (сопровождение и мониторинг механизмов безопасности, пересмотр и переоценка риска, управление документами и записями, корректирующие и превентивные меры, коммуникация рисков). Аутсорсинг процессов управления рисками.распределение ответственности за управление рисками. /Лек/	ОПК-13.1 ОПК-13.2 ОПК-15.3	Конспект (письменно). Компьютерные технологии
13	5	Текущий контроль	Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков. /Пр/	ОПК-15.2 ОПК-15.3 ОПК-13.1	Конспект (письменно). Дискуссия на практических занятиях
14	5	Текущий контроль	Обработка рисков информационной безопасности. Процесс обработки рисков. Способы обработки риска (принятие, уменьшение, передача, избежание риска). Оценка возврата инвестиций в информационную безопасность. План обработки рисков. /Лек/	ОПК-13.1 ОПК-13.2 ОПК-15.3	Конспект (письменно). Компьютерные технологии
15	6	Текущий контроль	Задание контрмер. Расчет риска реализации по всем угрозам для информационной системы после задания контрмер. Эффективность контрмеры. Эффективность комплекса контрмер. Расчет совокупной	ОПК-15.2 ОПК-15.3 ОПК-13.1	Конспект (письменно). Дискуссия на практических занятиях

			стоимости владения. Расчет возврата инвестиций. /Пр/		
16	6	Текущий контроль	Декларация о применимости механизмов контроля. /Ср/	ОПК-13.1 ОПК-13.2 ОПК-15.1 ОПК-15.2	Конспект (письменно). Компьютерные технологии
17			**Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.**		
18	7	Текущий контроль	Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками. /Лек/	ОПК-13.1 ОПК-13.2 ОПК-15.3	Конспект (письменно). Дискуссия на практических занятиях
19	7	Текущий контроль	Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы. /Пр/	ОПК-15.2 ОПК-15.3 ОПК-13.1	Конспект (письменно). Дискуссия на практических занятиях
20	8	Текущий контроль	Программные продуктыдля управления рисками информационнойбезопасности. /Ср/	ОПК-13.1 ОПК-13.2 ОПК-15.1 ОПК-15.2	Конспект (письменно). Компьютерные технологии
21	8	Текущий контроль	Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия. /Лек/	ОПК-13.1 ОПК-13.2 ОПК-15.3	Конспект (письменно). Компьютерные технологии
22	9	Текущий контроль	Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001. /Пр/	ОПК-15.2 ОПК-15.3 ОПК-13.1	Конспект (письменно). Дискуссия на практических занятиях
23	9	Текущий контроль	Законодательные и нормативные акты Российской Федерациив области защиты информации. /Ср/	ОПК-13.1 ОПК-13.2 ОПК-15.1 ОПК-15.2	Конспект (письменно). Компьютерные технологии
24	10	Текущий контроль	Изучение документов ГТК (защита от несанкционированного доступак информации). /Ср/	ОПК-13.1 ОПК-13.2 ОПК-15.1 ОПК-15.2	Конспект (письменно). Компьютерные технологии
25	11	Текущий контроль	BS ISO/IEC27001:2005 (BS 7799-2:2005). Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 779993:2006 ИISO/IEC 27005:2008 /Ср/	ОПК-13.1 ОПК-13.2 ОПК-15.1 ОПК-15.2	Конспект (письменно). Компьютерные технологии
26			**Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.**		Конспект (письменно). Дискуссия на практических занятиях
27	12	Текущий	Практические советы по внедрению	ОПК-13.1	Конспект (письменно).

		контроль	системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности. /Лек/	ОПК-13.2 ОПК-15.3	Компьютерные технологии
28	13	Текущий контроль	Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность. /Пр/	ОПК-15.2 ОПК-15. ОПК-15.3 ОПК-13.1	Конспект (письменно). Дискуссия на практических занятиях
29	14	Текущий контроль	Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта. /Лек/	ОПК-13.1 ОПК-13.2 ОПК-15.3	Конспект (письменно). Компьютерные технологии
30	15	Текущий контроль	Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта. /Пр/	ОПК-15.2 ОПК-15. ОПК-15.3 ОПК-13.1	Конспект (письменно). Дискуссия на практических занятиях
31	16	Текущий контроль	Проработка лекционного материала. Подготовка к промежуточному тестированию. /Ср/	ОПК-13.1 ОПК-13.2 ОПК-15.1 ОПК-15.2	Конспект (письменно). Компьютерные технологии
32	16	Тест			Тест Перечень вопросов к тестовому заданию.
33			Экзамен		Собеседование (устно), комплект экзаменационных билетов

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 так же краткая характеристика этих средств приведены в таблице

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

Критерии и шкалы оценивания компетенций в результате изучения дисциплины/ прохождении практики при проведении промежуточной аттестации в форме зачета и/или 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 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»	«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

Для оценочного средства «Тест» критерии и шкала оценивания устанавливаются разработчиком самостоятельно. В случае применения компьютерных технологий рекомендуется для проверки разных уровней сформированности компетенций (части компетенций, элементов компетенций) придерживаться следующих рекомендаций по выбору форм тестовых заданий:

Проверяемый уровень освоения компетенции/индикатора достижения компетенции	Количество тестовых заданий	Формы тестовых заданий
Минимальный	24	Тестовые задания с выбором одного правильного ответа из нескольких

		Тестовые задания с выбором нескольких правильных ответов из множества ответов
Базовый	16	Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры)
Высокий	10	Тестовые задания со свободно конструируемым ответом (интервью, эссе)

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

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:

Тема «Понятие риск. Информационные риски киберпространства».

1. Какой подход к оценке рисков используется в вашей организации?
2. Какие категории информационных рисков охватывает используемый вами подход?
3. Какие сотрудники вашей организации участвуют в процессах управления рисками и как распределяются между ними роли?

Кто и на основании какой информации принимает решения по обработке рисков?

4. К какой категории специалистов, с точки зрения отношения к оценке
5. рисков, вы сами относитесь?
6. Какие информационные риски представляют наибольшую опасность для вашей организации?

Тема «Основные элементы управления рисками информационной безопасности».

1. Какие процессы включает в себя система управления рисками и как эти процессы связаны с другими процессами системы управления (СУИР) ИБ?
2. Какие виды активов важнее для бизнеса вашей организации и почему?
3. Какие информационные риски вы рассматриваете в качестве основных?
4. В каких случаях область действия СУИР может охватывать не всю организацию?
5. Каковы отличительные признаки системного подхода к управлению рисками?
6. Какие виды нормативных и рабочих документов требуются для управления рисками в организации?
7. Каким образом могут распределяться обязанности и ответственность за управление рисками в организации?

Тема «Система управления информационными рисками».

1. Какие факторы влияют на решение о принятии риска?
2. На основании каких данных определяется вероятность угрозы?
3. Назовите основные источники уязвимостей.
4. Перечислите основные и вспомогательные бизнес-процессы ФГБОУ ВО ИрГУПС.
5. Какие этапы включает в себя оценка риска?

6. Какие параметры могут использоваться для описания бизнес-процессов организации?

7. Какие категории требований безопасности необходимо учитывать при оценке рисков?

8. Как можно определить ценность тех или иных активов?

9. Как связаны между собой оценка рисков и планирование непрерывности бизнеса?

Тема «Методические подходы к оценке информационных рисков хозяйствующих субъектов».

1. Раскройте сущность комплексной системы защиты информационных активов предприятий.

2. Опишите особенности система защиты информационных активов хозяйствующего субъекта.

3. Исследуйте особенности организационного направления в деятельности по защите информационных активов предприятия.

4. Охарактеризуйте сущность направления в организационной защите – работе с персоналом, определении его надежности.

5. Как осуществить оценку надежности персонала, как основного источника угроз информационным активам предприятия?

6. Суть методики оценки возможного ущерба при реализации угроз безопасности?

7. Охарактеризуйте сущность направления в организационной защите - информационно-аналитической деятельности по выявлению угроз информационным активам и управлению информационными рисками.

8. Обоснуйте позицию защищенности информационных активов с учетом информационных рисков в деятельности хозяйствующего субъекта.

9. Проведите сравнительный анализ нескольких наиболее известных методик оценки информационных рисков.

Тема «Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта».

1. Изложите суть экспертных методов по определению ценности защищаемых информационных активов.

2. Изложите суть методики оценки затрат на обеспечение информационной защищенности хозяйствующего субъекта.

3. Изложите суть эффективности оценки информационных рисков.

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 Комплект разно уровневых задач и заданий (контрольные задания).

Тема «Идентификация активов предприятия»

Важные активы внутри области действия системы управления информационной

безопасности (СУИБ) должны быть четко идентифицированы и должным образом оценены, а реестры, описывающие различные виды активов, должны быть взаимоувязаны и поддерживаться в актуальном состоянии. Для того чтобы быть уверенным в том, что ни один из активов не был пропущен или забыт, должна быть определена область действия СУИБ в терминах характеристик бизнеса, организации, ее расположения, ресурсов и технологий.

Идентификация активов включает:

- формирование модели бизнес-процессов;
- инвентаризация активов;
- формирование реестров активов;
- определение взаимосвязей между реестрами активов;
- построение модели активов;
- определение владельцев активов и их обязанностей;
- делегирование обязанностей по обеспечению безопасности активов;
- классификация и категорирование активов;
- определение правил допустимого использования активов.

Важно идентифицировать не только информационные активы, но другие активы, с которыми они связаны. Взаимосвязи между активами описываются моделью активов. Активы надо структурировать, категорировать и классифицировать по уровню конфиденциальности, критичности и другим признакам. Группирование похожих или связанных активов позволяет упростить процесс оценки рисков.

Нельзя обеспечить адекватный уровень информационной безопасности без установления подотчетности за активы.

Задание 1. Провести идентификацию активов предприятия/организации *(порядковый номер варианта выбрать в соответствии с номером учащегося в списке группы, либо выбрать организацию самостоятельно):*

1. Банк.
2. Супермаркет/магазин.
3. Научно-исследовательский институт.
4. Медицинское учреждение.
5. Торговая фирма.
6. Налоговая инспекция.
7. Агентство недвижимости.
8. Учебное заведение.
9. IT-компания.
10. Центр занятости населения.

Допускается осуществить идентификацию активов не всей организации (если она слишком велика), а один или несколько взаимодействующих между собой отделов/подразделений.

Задание 2. Осуществите расчет совокупной стоимости владения (ТСО).

Тема «Анализ угроз и уязвимостей»

Задание 1. Построить модель угроз информационной безопасности (ИБ) предприятия / организации / подразделения.

Задание 2. Описать уязвимости информационной безопасности.

Задание 3. Построить модель нарушителя ИБ.

Задание 4. Опишите профиль и жизненный цикл для одной из следующих угроз:

1. Заражение компьютерным вирусом.
2. Атака на отказ в обслуживании.
3. Несанкционированный доступ к системе и хищение конфиденциальной информации.
4. Выход из строя файлового сервера.
5. Пожар в офисе.

Постарайтесь дать как широкое определение угрозе, включающее в себя большое количество различных сценариев инцидентов, так и более узкое определение, включающее в себя лишь один конкретный сценарий реализации угрозы.

Задание 5. Оцените вероятности угроз.

Тема «Определение величины риска»

Задание 1. Постройте матрицу величины риска.

Задание 2. Откалибруйте шкалу оценки рисков.

Задание 3. Осуществите расчет риска информационной безопасности на основе модели угроз и уязвимостей.

Тема «Обработка рисков информационной безопасности»

Задание 1. Рассчитайте затраты на контрмеры (прямые и косвенные).

Задание 2. Осуществите расчет возврата инвестиций (ROI).

Задание 3. Подготовьте отчет об оценке рисков.

Отчет об оценке рисков необходим для руководства и всех заинтересованных сторон, вовлеченных в процесс управления рисками. Другими словами, этот документ нужен для коммуникации рисков.

Краткая структура отчета об оценке рисков:

1. Введение
2. Основания, общие сведения
3. Цели и задачи
4. Методология и результаты
5. Идентификация активов и требований
6. Оценка активов и последствий
7. Анализ угроз и уязвимостей
8. Вычисление и оценивание рисков
9. Резюме рисков для руководства

9. Описание самых высоких рисков и причин их существования

10. Приложения
11. Реестры активов, требований и рисков

Критерии и шкала оценивания разноуровневых задач и заданий

Оценка	Критерий оценки
«отлично»	Обучающийся полностью и правильно выполнил задания. Показал отличные знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Отчет оформлен аккуратно и в соответствии с предъявляемыми требованиями. Ответил на все дополнительные вопросы на защите
«хорошо»	Обучающийся выполнил задания с небольшими неточностями. Показал хорошие знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Есть недостатки в оформлении отчета. Ответил на большинство дополнительных вопросов на защите
«удовлетворительно»	Обучающийся выполнил задания с существенными неточностями. Показал удовлетворительные знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Качество оформления отчета имеет недостаточный уровень. При ответах на дополнительные вопросы на защите было допущено много неточностей
«неудовлетворительно»	При выполнении заданий обучающийся продемонстрировал недостаточный уровень знаний, умений и владения ими при решении задач в рамках усвоенного учебного материала. Обучающийся неспособен пояснить полученные результаты. При

	ответах на дополнительные вопросы на защите было допущено множество неточностей

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Критерии определения сформированности компетенций на различных этапах их формирования даны в пункте 1.2. Шкалы и критерии оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета, а также шкала для оценивания уровня освоения компетенций представлена в нижеследующей таблице.

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенций
«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 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»	«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	Компетенции не сформированы

3.1.4 Перечень теоретических вопросов к экзамену

1. Что такое информация ограниченного доступа?
2. В каких аспектах экономической деятельности, может выступать конфиденциальная информация?
3. Дайте характеристику понятия «информационные активы организации».
4. Какова взаимосвязь понятий «информационных активов» и «системы оценки рисков информационной безопасности хозяйствующего субъекта»?
5. Определите место и роль системы защиты информационных активов в системе управления деятельностью предприятия.
6. В чем заключается суть тревожных симптомов в сфере обеспечения безопасности информационных активов?
7. В чем заключается суть тенденции увеличения количества внутренних угроз, исходящих от сотрудников организаций (инсайдеров)?
8. Рассмотрите сущность основных видов организационных каналов несанкционированного доступа к информационным активам.
9. В чем заключается суть аналитической работы по обнаружению организационных каналов несанкционированного доступа к информационным активам?
10. Раскройте сущность комплексной системы защиты информационных активов предприятий.
11. Раскройте особенности система защиты информационных активов хозяйствующего субъекта.
12. Опишите особенности организационного направления в деятельности по защите информационных активов предприятия.
13. Охарактеризуйте сущность направления в организационной защите – работе с персоналом, определении его надежности.
14. Как осуществить оценку надежности персонала, как основного источника угроз информационным активам предприятия?
15. Опишите методику оценки возможного ущерба при реализации угроз безопасности.
16. Охарактеризуйте сущность направления в организационной защите - информационно-аналитической деятельности по выявлению угроз информационным активам и управлению информационными рисками.
17. Обоснуйте позицию защищенности информационных активов с учетом информационных рисков в деятельности хозяйствующего субъекта.
18. Проведите сравнительный анализ нескольких наиболее известных методик оценки информационных рисков.
19. Какие показатели включены в основу методики оценки информационных рисков предприятия?
20. Охарактеризуйте сущность методики и состав показателей типичной многофакторной модели оценки информационных рисков предприятия.
21. Охарактеризуйте сущность частной методики оценки надежности персонала в рамках общей методики многофакторной модели оценки информационных рисков предприятия.
22. Охарактеризуйте сущность частной методики оценки надежности технических и программно-аппаратных средств обработки информации.

23. Охарактеризуйте сущность частной методики организационно-режимных мер защиты с использованием программных комплексов анализа и управления рисками информационной системы «ГРИФ» и «КОНДОР».

24. Охарактеризуйте сущность экспертных методов по определению ценности защищаемых информационных активов.

25. Охарактеризуйте сущность методики оценки затрат на обеспечение информационной защищенности хозяйствующего субъекта.

26. Охарактеризуйте сущность эффективности оценки информационных рисков.

3.2 Тестирование по дисциплине

3.2.1 Структура фонда тестовых заданий по дисциплине

Структура фонда тестовых заданий по дисциплине
«Методология анализа информационных рисков»
Структура типового итогового теста по дисциплине за весь период ее освоения

Раздел дисциплины	*Тема раздела*	*Объект темы*	*Количество тестовых заданий (ТЗ), типы ТЗ*
Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия.	1.1 Информационные риски киберпространства (1.2 Государственное регулирование. Оценка рисков как основа корпоративного управления.	1.1.1 Кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов.	5 – тип А
		1.1.2Уровни оценки защищенности информации	5 – тип А
		1.1.3 Оценка рисков как основа корпоративного управления.	5 – тип А
	1.3 Идентификация активов.	1.2.1. Способы оценки информационных активов	5 – тип А
		1.2.2. Идентификация активов	4 – тип А 6 – тип В 6 – тип Д
		Итого по разделу	$\sum 36$ 24– тип А 6– тип В 6– тип Д
Раздел 2. Основные этапы и элементы управления рисками и их оценки.	2.1 Определение ценности активов (критерии оценки ущерба, таблица ценности активов.	2.1.1 Понятие риска. Подходы к управлению рисками.	5 – тип А
		2.1.2 Количественное и качественное определение величины риска.	5 – тип А
		2.1.3 Активы организации как ключевые факторы риска.	5 – тип А
	2.2 Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности	2.2.1 Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей.	5 – тип А 4 – тип Д
		2.2.2 Профиль и жизненный цикл угрозы..	4 – тип А 6 – тип В 2 – тип Д
		Итого по разделу	$\sum 36$ 24– тип А 6– тип В 6– тип Д
Раздел 3. Методические	3.1 Инструментальные средства для управления рисками.	3.1.1 Выбор инструментария для оценки рисков.	6 – тип А

подходы к оценке информационных рисков хозяйствующих субъектов.		3.1.2 Обзор методов и инструментальных средств управления рисками.	4 – тип С
	3.2 Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия.	3.2.1 Исследование организационной защиты информационных активов предприятия..	6 – тип А 4 – тип Д
		3.2.2 Оценка процессов СУИБ на соответствие ISO 27001	3 – тип А 4 – тип Д
		3.2.3 Законодательные и нормативные акты Российской Федерации в области защиты информации.	3 – тип А 6 – тип В
		Итого по разделу	$\sum 36$ 18– тип А 6– тип В 4– тип С 8– тип Д
Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.	4.1. Практические советы по внедрению системы управления рисками.	4.1.. Комплект типовых документов для управления рисками информационной безопасности.	1 – тип А
	4.2. Многофакторная модель хозяйствующего субъекта с учетом информационных рисков.	4.2.1 Укрупненная схема оценки защищенности информационных активов предприятия	1 – тип А
		4.2.2 Оценка рисков информационной безопасности предприятия	1 – тип А
	4.3.Управление информационными рисками	4.3.1 Создание комплексной системы защиты информационных активов хозяйствующего субъекта	1 – тип А 1 – тип Д
		4.3.2 Анализ ценности активов	1 – тип С 1 – тип Д
	4.4. Этапы оценки информационных рисков	4.4.1 Исследование ИС объекта	1 – тип А 1 – тип Д
		4.4.2 Предварительный анализ данных	1 – тип В 1 – тип Д
		4.4.3 Согласование объема и границ работ	1 – тип А 1 – тип Д
	4.5 Подготовительный этап	4.5.1 Необходимые мероприятия по исследованию ИС на проникновение	1 – тип А
		4.5.2. Анализ данных исследований	1– тип А 1– тип В 1– тип С 1– тип Д
	4.6 Рекомендации по повышению уровня защищенности	4.6.1 Основные требования по подготовке документов	1 – тип А
		4.6.2 Структура документа	1 – тип А
	4.7. Исследование программы оценки информационных рисков	4.7.1 Сбор и анализ данных	1 – тип А
		4.7.2 Мероприятия по проверке СЗИ ИС	1 – тип А

	4.8 Реализация программы обеспечения информационной безопасности компании	4.8.1 Подходы к созданию КСОИБ компании	1 – тип А
		4.8.2 Проектное задание	1– тип А 1– тип В 1– тип С 1– тип Д
	4.9 Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта	4.9.1 Эффективности вложений в информационную безопасность	2– тип А 1– тип В 1– тип С 1– тип Д
		4.9.2 Основные подходы к оценке затрат на ИБ	1– тип А 1– тип В 1– тип С 1– тип Д
		Итого по разделу	$\sum 36$ 17– тип А 5– тип В 5– тип С 9– тип Д
……...		***Итого по дисциплине***	$\sum 144$ 83– тип А 23– тип В 9– тип С 29– тип Д

Образец теста для проведения промежуточной аттестации в форме экзамена за А семестр по дисциплине «Методология анализа информационных рисков»
Вариант 1

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.

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.
Контрольное задание	Обучаемый самостоятельно или под руководством преподавателя выбирает контрольное задание, изучает материалы лекций и готовит ответ на задание. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
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

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 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

<table>
<tr>
<td>ИРГУПС
2021-2022
учебный год</td>
<td>Экзаменационный билет № 1
по дисциплине
«Б1. В.ДВ.08.01 «Методология анализа информационных рисков»

Специализация/профиль «Безопасность информационных систем и технологий»
8 семестр</td>
<td>Утверждаю:
Заведующий кафедрой
«ИСиЗИ» ИрГУПС
Т.К. Кириллова</td>
</tr>
<tr>
<td colspan="3">1. В чем заключается суть тенденции увеличения количества внутренних угроз, исходящих от сотрудников организаций (инсайдеров)?
2.Рассмотрите сущность основных видов организационных каналов несанкционированного доступа к информационным активам.
3.В чем заключается суть аналитической работы по обнаружению организационных каналов несанкционированного доступа к информационным активам?
Варианты размеров билета:
Билет формата А5 – 148*210мм
Билет формата А4 – 210*297мм</td>
</tr>
</table>