ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

Б1.О.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):
к.э.н., доцент, С.П. Серёдкин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «21» мая 2024 г. № 11

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

1 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 систем, проводить анализ уязвимостей	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 конфиденциальной информации применительно к видам тайны;

систем защиты информации автоматизированных систем		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
		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: -ь 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 безопасностью автоматизированных систем	Знать: - руководящие документы, по оценке угроз безопасности информации
		Уметь: - анализировать угрозы ИБ
		Владеть: - : способностью оценивать последствия от реализации угроз безопасности информации в автоматизированной системе

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма	*Код

		Семестр	Часы				индикатора достижения компетенции
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия.**						
1.1	Тема 1. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов).	8	4			6	ОПК-13.1 ОПК-13.2 ОПК-13.3
1.2	Тема 2. Идентификация активов (описание бизнес-процессов).	8		2			ОПК-13.1 ОПК-15.2 ОПК-15.3
2.0	**Раздел 2. Основные этапы и элементы управления рисками и их оценки.**						
2.1	Тема 3. Основные элементы управления рисками информационной безопасности.	8	4			4	ОПК-13.2 ОПК-13.3 ОПК-15.3
2.2	Тема 4. Определение ценности активов (критерии оценки ущерба, таблица ценности активов).	8		4			ОПК-15.1 ОПК-15.2
2.3	Тема 5. Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности.	8	4			4	ОПК-13.2 ОПК-13.3 ОПК-15.3
2.4	Тема 6. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	8		4			ОПК-15.1 ОПК-15.2
2.5	Тема 7. Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков.	8		4			ОПК-15.1 ОПК-15.2
2.6	Тема 8. Обработка рисков информационной безопасности. Оценка возврата инвестиций в информационную безопасность.	8	6			6	ОПК-13.2 ОПК-13.3 ОПК-15.3
2.7	Тема 9. Задание контрмер. Расчет риска реализации угроз. Эффективность контрмеры.	8		4			ОПК-15.1 ОПК-15.2
3.0	**Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.**						
3.1	Тема 10. Инструментальные средства для управления рисками.	8	4			4	ОПК-13.2 ОПК-13.3 ОПК-15.2
3.2	Тема 11. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса.	8		4			ОПК-15.1 ОПК-15.2
3.3	Тема 12. Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия.	8	4			4	ОПК-13.2 ОПК-13.3 ОПК-15.3
3.4	Тема 13. Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001.	8		4			ОПК-15.1 ОПК-15.2
3.5	Тема 14. Изучение документов ГТК (защита от несанкционированного доступа к информации).	8		4		4	ОПК-13.2 ОПК-13.3
4.0	**Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.**						
4.1	Тема 15. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	8	4			4	ОПК-13.2 ОПК-13.3 ОПК-15.3
4.2	Тема 16. Многофакторная модель оценки информационных рисков хозяйствующего субъекта.	8		4			ОПК-15.1 ОПК-15.2
4.3	Тема 17. Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта.	8	4			4	ОПК-13.2 ОПК-13.3 ОПК-15.3
	Форма промежуточной аттестации – экзамен	8	36				
	Итого часов (без учёта часов на промежуточную аттестацию)		34	34		40	

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

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

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Никитин, И. А. Процессы анализа и управления рисками в области ИТ : учебное пособие / И. А. Никитин, М. Т. Цулая. — 2-е изд., испр. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016. — 167 с. — URL: https://biblioclub.ru/index.php?page=book&id=429089 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Милославская, Н. Г. Управление рисками информационной безопасности: учебное пособие для вузов : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия – Телеком, 2013. — 130 с. — URL: https://biblioclub.ru/index.php?page=book&id=253576 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Аверченков, В. И. Аудит информационной безопасности : учебное пособие / В. И. Аверченков. — 4-е изд., стер. — Москва : ФЛИНТА, 2021. — 269 с. — URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.2.2	Анисимов, А. А. Менеджмент в сфере информационной безопасности: курс лекций : курс лекций / А. А. Анисимов. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ)|Бином. Лаборатория знаний, 2009. — 176 с. — URL: https://biblioclub.ru/index.php?page=book&id=232981 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.2.3	Балдин, К. В. Управление рисками в инновационно-инвестиционной деятельности предприятия : учебное пособие / К. В. Балдин, И. И. Передеряев, Р. С. Голов. — 6-е изд., стер. — Москва : Дашков и К°, 2023. — 418 с. — URL: https://biblioclub.ru/index.php?page=book&id=710924 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.2.4	Глухов, Н. И. Оценка информационных рисков предприятия : учеб. пособие / Н. И. Глухов ; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ. — Иркутск : ИрГУПС, 2013. — 148 с. — Текст : непосредственный.	62

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 направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, специализация – Безопасность открытых информационных систем / С.П. Серёдкин ; ИрГУПС. – Иркутск : ИрГУПС, 2024. – 12 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47641_1529_2024_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 занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «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	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

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

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией 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.

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

Дисциплина «Методология анализа информационных рисков» участвует в формировании компетенций:

ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем

ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
8 семестр				
1.0	**Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия**			
1.1	Текущий контроль	Тема 1. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов).	ОПК-13.1 ОПК-13.2 ОПК-13.3	Конспект (письменно) Тестирование (компьютерные технологии)
1.2	Текущий контроль	Тема 2. Идентификация активов (описание бизнес-процессов).	ОПК-13.1 ОПК-15.2 ОПК-15.3	Дискуссия (устно) Конспект (письменно)
2.0	**Раздел 2. Основные этапы и элементы управления рисками и их оценки**			
2.1	Текущий контроль	Тема 3. Основные элементы управления рисками информационной безопасности.	ОПК-13.2 ОПК-13.3 ОПК-15.3	Конспект (письменно) Тестирование (компьютерные технологии)
2.2	Текущий контроль	Тема 4. Определение ценности активов (критерии оценки ущерба, таблица ценности активов).	ОПК-15.1 ОПК-15.2	Дискуссия (устно) Конспект (письменно)
2.3	Текущий контроль	Тема 5. Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности.	ОПК-13.2 ОПК-13.3 ОПК-15.3	Конспект (письменно) Тестирование (компьютерные технологии)
2.4	Текущий контроль	Тема 6. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	ОПК-15.1 ОПК-15.2	Дискуссия (устно) Конспект (письменно)
2.5	Текущий контроль	Тема 7. Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков.	ОПК-15.1 ОПК-15.2	Дискуссия (устно) Конспект (письменно)
2.6	Текущий контроль	Тема 8. Обработка рисков информационной безопасности. Оценка возврата инвестиций в информационную безопасность.	ОПК-13.2 ОПК-13.3 ОПК-15.3	Конспект (письменно) Тестирование (компьютерные технологии)
2.7	Текущий контроль	Тема 9. Задание контрмер. Расчет риска реализации угроз. Эффективность контрмеры.	ОПК-15.1 ОПК-15.2	Дискуссия (устно) Конспект (письменно)
3.0	**Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов**			
3.1	Текущий контроль	Тема 10. Инструментальные	ОПК-13.2	Дискуссия (устно)

		средства для управления рисками.	ОПК-13.3 ОПК-15.2	Конспект (письменно) Тестирование (компьютерные технологии)
3.2	Текущий контроль	Тема 11. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса.	ОПК-15.1 ОПК-15.2	Дискуссия (устно) Конспект (письменно)
3.3	Текущий контроль	Тема 12. Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия.	ОПК-13.2 ОПК-13.3 ОПК-15.3	Конспект (письменно) Тестирование (компьютерные технологии)
3.4	Текущий контроль	Тема 13. Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001.	ОПК-15.1 ОПК-15.2	Дискуссия (устно) Конспект (письменно)
3.5	Текущий контроль	Тема 14. Изучение документов ГТК (защита от несанкционированного доступа к информации).	ОПК-13.2 ОПК-13.3	Конспект (письменно)
4.0	**Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта**			
4.1	Текущий контроль	Тема 15. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	ОПК-13.2 ОПК-13.3 ОПК-15.3	Конспект (письменно) Тестирование (компьютерные технологии)
4.2	Текущий контроль	Тема 16. Многофакторная модель оценки информационных рисков хозяйствующего субъекта.	ОПК-15.1 ОПК-15.2	Дискуссия (устно) Конспект (письменно)
4.3	Текущий контроль	Тема 17. Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта.	ОПК-13.2 ОПК-13.3 ОПК-15.3	Дискуссия (устно) Конспект (письменно) Тестирование (компьютерные технологии)
	Промежуточная аттестация	По всем разделам		Экзамен (собеседование) Экзамен - тестирование (компьютерные технологии)

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

Описание показателей и критериев оценивания компетенций. Описание шкал оценивания

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

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

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

Перечень оценочных средств, используемых для оценивания компетенций, а также

краткая характеристика этих средств приведены в таблице.

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Дискуссия	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения. Может быть использовано для оценки знаний и умений обучающихся	Перечень дискуссионных тем
2	Конспект	Особый вид текста, в основе которого лежит аналитико-синтетическая переработка информации первоисточника (исходного текста). Цель этой деятельности — выявление, систематизация и обобщение (с возможной критической оценкой) наиболее ценной (для конспектирующего) информации. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы конспектов
3	Тестирование (компьютерные технологии)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

Промежуточная аттестация

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

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

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий

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

Тест – промежуточная аттестация в форме экзамена

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

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Дискуссия

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Выбранная обучающимся тема (проблема) актуальна в данном курсе; представлен подробный план-конспект, в котором отражены вопросы для дискуссии; временной регламент обсуждения обоснован; даны возможные варианты ответов; использованы примеры из науки и практики
«хорошо»		Выбранная обучающимся тема (проблема) актуальна в данном курсе; представлен сжатый план-конспект, в котором отражены вопросы для дискуссии; временной регламент обсуждения обоснован; отсутствуют возможные варианты ответов; приведен один пример из практики
«удовлетворительно»		Выбранная обучающимся тема (проблема) недостаточно актуальна в данном курсе; представлен содержательно краткий план-конспект, в котором отражены вопросы для дискуссии; отсутствует временной регламент обсуждения; отсутствуют возможные варианты ответов; отсутствуют примеры из практики
«неудовлетворительно»	«не зачтено»	Выбранная обучающимся тема (проблема) не актуальна для данного курса; частично представлены вопросы для дискуссии; отсутствует временной регламент обсуждения; отсутствуют возможные варианты ответов; отсутствуют примеры из практики

Конспект

Шкалы оценивания	Критерии оценивания

«отлично»	«зачтено»	Конспект по теме выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся по заданной теме в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; раскрыл тему полностью и ответил на все вопросы преподавателя по конкретной теме конспекта. Конспект оформлен аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»		Конспект по теме выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся по заданной теме в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; раскрыл тему не полностью и ответил на часть вопросов преподавателя по конкретной теме конспекта. Конспект оформлен аккуратно, с незначительными исправлениями
«удовлетворительно»		Конспект по теме выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся по заданной теме в не полном объеме с частичным соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; раскрыл тему не полностью и ответил на часть вопросов преподавателя по конкретной теме конспекта. Конспект оформлен не аккуратно
«неудовлетворительно»	«не зачтено»	Конспект по теме не выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся не по заданной теме в не полном объеме без соблюдения необходимой последовательности. Обучающийся работал не самостоятельно; не раскрыл тему и не ответил на вопросы преподавателя по конкретной теме конспекта. Конспект оформлен не аккуратно

Тестирование

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

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

3.1 Типовые контрольные задания для проведения дискуссии

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

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.

Образец типового варианта вопросов для проведения собеседования

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

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.

Образец типового варианта вопросов для проведения собеседования

Тема 1. «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?

Образец типового варианта вопросов для проведения собеседования

Тема 2. «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?

Образец типового варианта вопросов для проведения собеседования

Тема 3. Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности.

1. Вопрос: Какие основные категории угроз информационной безопасности существуют, и как они могут повлиять на организацию?
2. Вопрос: Что такое уязвимость информационной безопасности и каковы основные типы уязвимостей, встречающиеся в современных информационных системах?

3. Вопрос: Как можно классифицировать угрозы информационной безопасности по степени их воздействия и вероятности возникновения? Приведите примеры для каждой категории.

4. Вопрос: Какие меры могут быть предприняты для минимизации рисков, связанных с типовыми уязвимостями информационной безопасности?

Образец типового варианта вопросов для проведения собеседования

Тема 4. Обработка рисков информационной безопасности. Процесс обработки рисков. Способы обработки риска (принятие, уменьшение, передача, избежание риска). Оценка возврата инвестиций в информационную безопасность. План обработки рисков.

1. Вопрос: Какие основные этапы включает процесс обработки рисков информационной безопасности и в чем заключается каждый из них?

2. Вопрос: Какие способы обработки рисков информационной безопасности существуют, и в каких ситуациях каждый из них может быть применен?

3. Вопрос: Как оценивается возврат инвестиций в информационную безопасность и какие метрики используются для этого?

4. Вопрос: Что включает в себя план обработки рисков и какие ключевые элементы необходимо учитывать при его разработке?

Образец типового варианта вопросов для проведения собеседования

Тема 5. Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками.

1. Вопрос: Какие критерии необходимо учитывать при выборе инструментальных средств для управления рисками информационной безопасности?

2. Вопрос: Какие методы оценки рисков используются в информационной безопасности и как они применяются на практике?

3. Вопрос: Какие инструментальные средства для управления рисками наиболее популярны на рынке, и каковы их основные функции?

4. Вопрос: Как интеграция инструментальных средств управления рисками может улучшить процесс управления информационной безопасностью в организации?

Образец типового варианта вопросов для проведения собеседования

Тема 6. Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия.

1. Вопрос: Какие современные методические подходы используются для обеспечения защищенности информационных активов предприятия?

2. Вопрос: Как методологии управления информационной безопасностью, такие как ISO/IEC 27001 и NIST, помогают в защите информационных активов?

3. Вопрос: Какие преимущества и недостатки различных методических подходов к обеспечению информационной безопасности можно выделить?

4. Вопрос: Как адаптация современных методических подходов к специфике конкретного предприятия влияет на эффективность обеспечения информационной безопасности?

Образец типового варианта вопросов для проведения собеседования

Тема 7. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.

1. Вопрос: Какие шаги необходимо предпринять для успешного внедрения системы управления рисками информационной безопасности в организации?

2. Вопрос: Какие типовые документы необходимы для управления рисками информационной безопасности и какова их основная роль?

3. Вопрос: Какие практические советы можно дать для повышения эффективности системы управления рисками на этапе ее внедрения?

4. Вопрос: Как обеспечить постоянное обновление и актуализацию документации по управлению рисками информационной безопасности?

Образец типового варианта вопросов для проведения собеседования

Тема 8. Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта.

1. Вопрос: Какие методические подходы используются для оценки затрат на обеспечение защищенности информационных активов хозяйствующего субъекта?
2. Вопрос: Как производится расчет стоимости мер по обеспечению информационной безопасности в рамках различных методологических подходов?
3. Вопрос: Какие факторы следует учитывать при оценке затрат на информационную безопасность для максимизации эффективности инвестиций?
4. Вопрос: Как сравнивать и анализировать различные методические подходы к оценке затрат на информационную безопасность для выбора оптимального решения?

3.2 Комплект разноуровневых задач и заданий (контрольные задания).

Тема 1. «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 2. Определение ценности активов (критерии оценки ущерба, таблица ценности активов).

Важные активы внутри области действия системы управления информационной безопасностью (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.

Для определения ценности активов необходимо учитывать критерии оценки ущерба, которые могут включать:

- финансовые потери;
- репутационный ущерб;
- утрату конфиденциальности данных;
- нарушение деловых процессов;
- правовые и регуляторные последствия.

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):

- Банк.
- Супермаркет/магазин.
- Научно-исследовательский институт.
- Медицинское учреждение.
- Торговая фирма.
- Налоговая инспекция.
- Агентство недвижимости.
- Учебное заведение.
- IT-компания.
- Центр занятости населения.

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

Задание 2: Составить таблицу ценности активов, включив в нее следующие параметры:

- Наименование актива.
- Владелец актива.
- Категория актива (информационный, физический и т.д.).
- Критичность актива (высокая, средняя, низкая).

- Уровень конфиденциальности (высокий, средний, низкий).
- Возможный ущерб в случае компрометации (финансовый, репутационный и т.д.).

Тема 3. «Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.»

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 4. «Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков»

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 5. «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.»

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

Тема 6. «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»

Важные активы внутри области действия системы управления информационной безопасностью (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.

Для определения ценности активов необходимо учитывать критерии оценки ущерба, которые могут включать:

- финансовые потери;
- репутационный ущерб;
- утрату конфиденциальности данных;
- нарушение деловых процессов;
- правовые и регуляторные последствия.

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:

- Идентификация базовых угроз: Определить три основные угрозы, которые могут нанести вред ресурсу.
- Оценка вероятности реализации угроз: Оценить вероятность реализации каждой угрозы, используя шкалу от 1 до 5, где 1 – очень низкая вероятность, а 5 – очень высокая.
- Оценка последствий: Определить потенциальные последствия каждой угрозы для ресурса. Включить в анализ как непосредственные, так и косвенные последствия.
- Расчет риска реализации: Рассчитать риск реализации каждой угрозы по формуле: Риск = Вероятность × Последствия.
- Оценка общего риска: Проанализировать полученные результаты и определить общий риск для ресурса.

Задание 2:

- Сравнение рисков: Сопоставить рассчитанный риск реализации каждой угрозы и определить наиболее значимые из них.
- Планирование мер по снижению риска: На основе результатов анализа разработать стратегии и меры по снижению риска реализации угроз для ресурса.
- Мониторинг и адаптация: Определить механизмы мониторинга и адаптации стратегий снижения риска с течением времени и изменением обстановки.

Тема 7. Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001.

Описание (раздел):

В данном разделе проводится исследование системы управления информационной безопасностью (СУИБ) предприятия с целью оценки ее соответствия требованиям международного стандарта ISO 27001. Оценка включает в себя анализ организационных мероприятий, политик, процедур и практик, направленных на защиту информационных активов.

Задание 1:

- Идентификация информационных активов: Определить все информационные активы предприятия, включая данные, системы, программное обеспечение и инфраструктуру.
- Анализ организационных мероприятий: Изучить существующие организационные меры по защите информационных активов, включая политики, процедуры и контрольные механизмы.
- Оценка соответствия требованиям ISO 27001: Провести сравнительный анализ между текущими организационными мероприятиями и требованиями стандарта ISO 27001.
- Выявление пробелов и слабых мест: Определить области, где существует несоответствие с требованиями стандарта или потенциальные уязвимости в системе управления информационной безопасностью.

Задание 2:

- Разработка рекомендаций по улучшению: На основе выявленных проблемных областей разработать рекомендации по улучшению системы управления информационной безопасностью.
- Планирование мероприятий по приведению в соответствие: Составить план действий для внедрения рекомендаций и устранения выявленных несоответствий с требованиями ISO 27001.
- Внедрение улучшений и мониторинг: Организовать внедрение предложенных улучшений и внести изменения в процессы управления информационной безопасностью. Установить механизмы мониторинга и регулярного аудита для обеспечения непрерывного соответствия стандарту.

Тема 8. Изучение документов ГТК (защита от несанкционированного доступа к информации).

Описание (раздел):

Этот раздел посвящен изучению документов государственной тайны и конфиденциальной информации (ГТК) с целью обеспечения защиты от несанкционированного доступа к информации. В рамках данного исследования анализируются требования, положения и меры по защите информации, установленные соответствующими нормативными актами.

Задание 1:

- Изучение документов ГТК: Ознакомиться с основными документами, регулирующими вопросы защиты государственной тайны и конфиденциальной информации, включая законы, постановления, приказы и инструкции.
- Анализ требований к защите информации: Выявить основные требования и положения, касающиеся защиты информации от несанкционированного доступа, предусмотренные документами ГТК.
- Оценка актуальности и соответствия: Проанализировать, насколько текущие политики и практики по защите информации соответствуют требованиям и рекомендациям, изложенным в документах ГТК.
- Выявление пробелов и уязвимостей: Определить возможные пробелы в системе защиты информации и уязвимости, которые могут привести к несанкционированному доступу.

Задание 2:

- Разработка мер по улучшению: На основе выявленных проблемных областей

разработать меры по улучшению системы защиты информации с учетом требований документов ГТК.

- Планирование и внедрение мероприятий: Составить план действий для внедрения предложенных мер по улучшению защиты информации от несанкционированного доступа.
- Обучение персонала: Организовать обучение персонала по правилам и процедурам защиты информации, установленным в документах ГТК.
- Мониторинг и адаптация: Установить механизмы мониторинга и адаптации политики защиты информации с учетом изменений в законодательстве и обстановке в области информационной безопасности.

Тема 9. «Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность».

Описание (раздел):

В данном разделе рассматривается многофакторная модель оценки информационных рисков для хозяйствующего субъекта. Представлена укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков, включающая подготовительный этап, оценку рисков, управление рисками, создание комплексной системы защиты информационных активов, реализацию программы обеспечения информационной безопасности и анализ эффективности вложений.

Задание 1:

- Подготовительный этап: Определить цели и задачи оценки информационных рисков, а также сформировать команду и ресурсы для выполнения оценки.
- Оценка рисков информационной безопасности предприятия: Проанализировать возможные угрозы и уязвимости информационных активов, определить потенциальные последствия инцидентов безопасности и вероятность их возникновения.
- Управление информационными рисками: Разработать стратегии по снижению рисков, включая технические и организационные меры.
- Создание комплексной системы защиты информационных активов хозяйствующего субъекта: Разработать и внедрить систему политик, процедур и технологий, направленных на обеспечение безопасности информации.

Задание 2:

- Реализация программы обеспечения информационной безопасности компании: Организовать внедрение предложенных мер по защите информации и обучить персонал основам информационной безопасности.
- Анализ эффективности вложений в информационную безопасность: Оценить результаты реализации программы обеспечения информационной безопасности и определить эффективность вложений, сравнив исходные и полученные уровни защищенности информации.
- Непрерывное управление рисками: Установить механизмы регулярного мониторинга информационных рисков и их изменений, проводить анализ новых угроз и обновлять стратегии защиты соответственно.
- Постоянное совершенствование системы защиты: Проводить аудиты и ревизии системы защиты информационных активов, выявлять слабые места и улучшать меры безопасности в соответствии с изменяющейся угрозовой средой.
- Создание культуры безопасности: Пропагандировать осознание и значимость информационной безопасности среди сотрудников предприятия, обучать их правилам и процедурам безопасности и повышать общую грамотность в этой области.
- Взаимодействие с внешними структурами: Сотрудничать с соответствующими

органами и специалистами в области информационной безопасности для обмена опытом, получения консультаций и участия в мероприятиях по повышению уровня защиты.

3.3 Типовые контрольные задания для проведения тестирования

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

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-13.1 ОПК-13.2 ОПК-13.3	Тема 1. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов).	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-13.1 ОПК-15.2 ОПК-15.3	Тема 2. Идентификация активов (описание бизнес-процессов).	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-13.2 ОПК-13.3 ОПК-15.3	Тема 3. Основные элементы управления рисками информационной безопасности.	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-15.1 ОПК-15.2	Тема 4. Определение ценности активов (критерии оценки ущерба, таблица ценности активов).	Знание	4 – ОТЗ 4 – ЗТЗ
		Умение	4 – ОТЗ 4 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-13.2 ОПК-13.3 ОПК-15.3	Тема 5. Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности.	Знание	4 – ОТЗ 4 – ЗТЗ
		Умение	4 – ОТЗ 4 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-15.1 ОПК-15.2	Тема 6. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	Знание	4 – ОТЗ 4 – ЗТЗ
		Умение	4 – ОТЗ 4 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-15.1 ОПК-15.2	Тема 7. Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-13.2 ОПК-13.3 ОПК-15.3	Тема 8. Обработка рисков информационной безопасности. Оценка возврата инвестиций в информационную безопасность.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-15.1 ОПК-15.2	Тема 9. Задание контрмер. Расчет риска реализации угроз. Эффективность контрмеры.	Знание	3 – ОТЗ 3 – ЗТЗ

		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-13.2 ОПК-13.3 ОПК-15.2	Тема 10. Инструментальные средства для управления рисками.	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-15.1 ОПК-15.2	Тема 11. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса.	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-13.2 ОПК-13.3 ОПК-15.3	Тема 12. Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия.	Знание	4 – ОТЗ 4 – ЗТЗ
		Умение	4 – ОТЗ 4 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-15.1 ОПК-15.2	Тема 13. Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001.	Знание	4 – ОТЗ 4 – ЗТЗ
		Умение	4 – ОТЗ 4 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-13.2 ОПК-13.3	Тема 14. Изучение документов ГТК (защита от несанкционированного доступа к информации).	Знание	4 – ОТЗ 4 – ЗТЗ
		Умение	4 – ОТЗ 4 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-13.2 ОПК-13.3 ОПК-15.3	Тема 15. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-15.1 ОПК-15.2	Тема 16. Многофакторная модель оценки информационных рисков хозяйствующего субъекта.	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-13.2 ОПК-13.3 ОПК-15.3	Тема 17. Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта.	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
		Итого	106 – ОТЗ 106 – ЗТЗ

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

Вопросы с выбором ответа из списка (50 вопросов)

1. Что является основным фактором информационного риска?

a) Пользователи
b) Активы
c) Политики
d) Процедуры

2. Какой из следующих методов используется для оценки рисков?

a) SWOT-анализ
b) PEST-анализ
c) Количественный анализ
d) Анализ 5 сил Портера

3. Что включает в себя процесс управления рисками?

a) Идентификация, оценка, контроль
b) Анализ, планирование, исполнение
c) Проектирование, разработка, тестирование
d) Мониторинг, отчетность, аудит

4. Какой из следующих методов лучше всего подходит для оценки финансовых потерь от информационных рисков?

a) Качественный анализ
b) Количественный анализ
c) Сценарный анализ
d) Анализ на основе мнений экспертов

5. Что такое кибертерроризм?

a) Неавторизованный доступ к данным
b) Использование интернета для нанесения ущерба или запугивания
c) Вирусное заражение системы
d) Потеря данных из-за аппаратного сбоя

6. Как называется процесс уменьшения риска до приемлемого уровня?

a) Принятие риска
b) Избежание риска
c) Уменьшение риска
d) Передача риска

7. Какие из следующих уязвимостей относятся к программному обеспечению?

a) Недостаток в разработке
b) Физический доступ
c) Социальная инженерия
d) Незащищенные коммуникации

8. Что из ниже перечисленного относится к типовым угрозам информационной безопасности?

a) Сильные пароли
b) Вирусы и трояны
c) Шифрование данных
d) Регулярные обновления

9. Какой из следующих методов лучше всего подходит для передачи риска?

a) Закупка страховки
b) Обновление программного обеспечения
c) Установка межсетевых экранов
d) Обучение персонала

10. Какой стандарт часто используется для управления информационной безопасностью?

a) ISO 9001
b) ISO 14001
c) ISO 27001
d) ISO 45001

11. Что является примером активов организации?

a) Сотрудники
b) Политики
c) Данные
d) Методы

12. Какое из следующих определений наиболее точно описывает понятие риска?

a) Потенциальная угроза
b) Вероятность потери
c) Мера воздействия
d) Неизвестный фактор

13. Что такое оценка возврата инвестиций в информационную безопасность?

a) Анализ затрат на безопасность
b) Определение эффективности мер безопасности
c) Оценка потенциальных убытков
d) Расчет времени восстановления

14. Какой из следующих документов является ключевым для управления рисками?

a) Политика безопасности
b) План восстановления после сбоев
c) План обработки рисков
d) Инструкции по использованию

15. Что из ниже перечисленного является государственным регулированием в области информационной безопасности?

a) Закон о защите данных
b) Корпоративные политики
c) Технические стандарты
d) Обучение сотрудников

16. Какие активы считаются ключевыми факторами риска?

a) Технологии и оборудование
b) Финансовые ресурсы
c) Клиенты и партнеры
d) Информационные системы и данные

17. Что такое сценарный анализ в оценке рисков?

a) Метод прогнозирования
b) Оценка финансовых потерь
c) Разработка гипотетических ситуаций
d) Моделирование угроз

18. Какие методы используются для уменьшения информационных рисков?

a) Шифрование данных
b) Обучение персонала
c) Установка антивирусного ПО
d) Все выше перечисленное

19. Что из ниже перечисленного относится к методам качественной оценки рисков?

a) Моделирование угроз
b) Анкетирование
c) Статистический анализ
d) Анализ потерь

20. Как называется процесс передачи риска третьей стороне?

a) Принятие риска
b) Избежание риска
c) Передача риска
d) Уменьшение риска

21. Что является основным инструментом для мониторинга рисков?

a) Дашборды и отчеты
b) Политики безопасности
c) Антивирусное ПО
d) Шифрование данных

22. Какие из перечисленных угроз можно считать внутренними?

a) Вирусы и трояны
b) Сотрудники и контрагенты
c) Взломы и атаки
d) Спам и фишинг

23. Какой из методов оценки рисков предполагает использование мнений экспертов?

a) Качественный анализ
b) Количественный анализ
c) SWOT-анализ
d) Анализ методом Delphi

24. Что из ниже перечисленного включает в себя план обработки рисков?

a) Политики и процедуры
b) Меры по снижению рисков
c) Оценка потенциальных убытков

d) Анализ активов

25. Что является ключевым элементом оценки затрат на обеспечение защищенности информационных активов?

a) Финансовый анализ
b) Технический анализ
c) Анализ угроз
d) Анализ уязвимостей

26. Как называется процесс принятия остаточного риска после применения всех мер безопасности?

a) Принятие риска
b) Избежание риска
c) Уменьшение риска
d) Передача риска

27. Что из ниже перечисленного лучше всего описывает концепцию "актив"?

a) Оборудование
b) Сотрудники
c) Данные
d) Все вышеперечисленное

28. Какие из перечисленных методов применимы для количественной оценки рисков?

a) Моделирование сценариев
b) Анализ затрат и выгод
c) Статистический анализ
d) Все вышеперечисленное

29. Какой из следующих методов управления рисками связан с внедрением новых технологий?

a) Принятие риска
b) Избежание риска
c) Уменьшение риска
d) Передача риска

30. Что является основным преимуществом использования инструментальных средств управления рисками?

a) Экономия времени и ресурсов
b) Повышение надежности данных
c) Уменьшение количества ошибок
d) Все вышеперечисленное

31. Что из ниже перечисленного относится к внешним угрозам информационной безопасности?

a) Сотрудники
b) Партнеры
c) Хакеры

d) Контрагенты

32. Какие из перечисленных методов включают в себя качественный анализ рисков?

a) SWOT-анализ
b) Моделирование угроз
c) Анкетирование
d) Все вышеперечисленное

33. Какой из ниже перечисленных факторов чаще всего вызывает уязвимости в информационной безопасности?

a) Недостаток финансирования
b) Недостаток образования
c) Недостаток обновлений
d) Недостаток контроля

34. Какие из перечисленных факторов чаще всего учитываются при оценке рисков?

a) Вероятность и воздействие
b) Финансовые показатели
c) Уровень угроз
d) Доступность ресурсов

35. Какой из ниже перечисленных методов используется для оценки угроз?

a) Моделирование сценариев
b) Анкетирование
c) Статистический анализ
d) Все вышеперечисленное

Как называется процесс идентификации и анализа возможных угроз?

a) Оценка угроз
b) Управление угрозами
c) Моделирование угроз
d) Аудит угроз

36. Какой из ниже перечисленных элементов не относится к активам организации?

a) Программное обеспечение
b) Финансовые отчеты
c) Персональные данные сотрудников
d) Внешние поставщики

37. Какое из следующих определений описывает понятие уязвимости?

a) Потенциальная угроза
b) Недостаток или слабое место
c) Вероятность возникновения инцидента
d) Последствия угрозы

Что является основным методом управления уязвимостями?

a) Регулярные обновления программного обеспечения
b) Обучение сотрудников

c) Внедрение политик безопасности
d) Все вышеперечисленное

38. Какой из следующих методов лучше всего подходит для оценки эффективности мер безопасности?

a) Аудит безопасности
b) Мониторинг сети
c) Тестирование на проникновение
d) Все вышеперечисленное

39. Какой из ниже перечисленных факторов чаще всего влияет на успешность управления рисками?

a) Поддержка руководства
b) Финансирование
c) Технические ресурсы
d) Обучение сотрудников

40. Какой из методов используется для анализа уязвимостей?

a) Пентест
b) Анкетирование
c) Анализ цепочки поставок
d) Все вышеперечисленное

41. Какой из следующих подходов к управлению рисками включает перенос риска на третью сторону?

a) Принятие риска
b) Избежание риска
c) Уменьшение риска
d) Передача риска

42. Что является ключевым элементом плана восстановления после сбоев?

a) Обеспечение резервного копирования
b) Тестирование планов
c) Обучение персонала
d) Все вышеперечисленное

43. Что из перечисленного относится к организационным мерам безопасности?

a) Политики и процедуры
b) Антивирусное ПО
c) Межсетевые экраны
d) Шифрование данных

44. Какой из ниже перечисленных методов используется для управления изменениями в системе безопасности?

a) Планирование изменений
b) Оценка рисков
c) Тестирование изменений
d) Все вышеперечисленное

45. Что является основной целью аудита информационной безопасности?

a) Оценка текущего состояния безопасности
b) Выявление уязвимостей
c) Разработка рекомендаций
d) Все вышеперечисленное

46. Какой из ниже перечисленных факторов наиболее важен при оценке рисков?

a) Вероятность
b) Влияние
c) Стоимость
d) Все вышеперечисленное

47. Что является ключевым этапом управления инцидентами безопасности?

a) Идентификация инцидентов
b) Реакция на инциденты
c) Восстановление после инцидентов
d) Все вышеперечисленное

48. Какой из методов управления рисками предполагает полный отказ от активности, вызывающей риск?

a) Принятие риска
b) Избежание риска
c) Уменьшение риска
d) Передача риска

Вопросы с написанием правильного ответа (50 вопросов)

1. Опишите основные элементы управления рисками информационной безопасности.
2. Приведите примеры количественного и качественного определения величины риска.
3. Назовите активы организации, которые могут быть ключевыми факторами риска.
4. Охарактеризуйте подходы к управлению рисками.
5. Перечислите типовые угрозы информационной безопасности.
6. Определите основные уязвимости информационной безопасности.
7. Опишите процесс обработки рисков информационной безопасности.
8. Какие существуют способы обработки риска?
9. Объясните, что такое оценка возврата инвестиций в информационную безопасность.
10. Разработайте план обработки рисков для конкретного информационного актива.
11. Какие инструментальные средства можно использовать для управления рисками?
12. Как осуществляется выбор инструментария для оценки рисков?
13. Приведите обзор методов управления рисками.
14. Как анализируются современные методические подходы к обеспечению защищенности информационных активов предприятия?
15. Опишите методику оценки информационных рисков хозяйствующего субъекта.
16. Какие документы необходимы для управления рисками информационной безопасности?
17. Приведите примеры методических подходов к оценке затрат на обеспечение защищенности информационных активов.
18. Разработайте проект внедрения системы управления информационными рисками для выбранного предприятия.
19. Как оценить эффективность существующей системы управления информационными рисками на предприятии?
20. Составьте план обучения сотрудников по вопросам управления информационными рисками.
21. Опишите процесс анализа влияния внешних факторов на систему управления информационными рисками предприятия.

22. Разработайте систему мониторинга и контроля за реализацией мер по управлению информационными рисками.
23. Как провести аудит уязвимостей информационной безопасности на предприятии?
24. Перечислите меры по снижению типовых угроз информационной безопасности.
25. Определите методы обработки рисков и оцените их эффективность.
26. Какие основные этапы включает в себя управление рисками?
27. Опишите процесс идентификации рисков.
28. Как осуществляется анализ рисков?
29. Разработайте план реагирования на инциденты информационной безопасности.
30. Объясните роль руководства в управлении информационными рисками.
31. Приведите примеры использования страхования для передачи риска.
32. Как осуществляется мониторинг и отчетность в управлении рисками?
33. Опишите методику оценки остаточного риска.
34. Как проводится регулярная оценка рисков?
35. Перечислите методы предотвращения кибертерроризма.
36. Какие факторы влияют на выбор метода оценки рисков?
37. Опишите процесс аудита информационной безопасности.
38. Как осуществляется анализ сценариев в оценке рисков?
39. Какие меры могут быть приняты для защиты промышленных систем?
40. Как организовать защиту информации при использовании электронных отчетов?
41. Опишите процесс внедрения политик безопасности.
42. Как проводится тестирование на проникновение?
43. Какие методы используются для анализа цепочки поставок в контексте управления рисками?
44. Как осуществляется контроль за соблюдением политик безопасности?
45. Какие меры необходимо предпринять для защиты информации при удаленной работе сотрудников?
46. Опишите процесс управления изменениями в системе безопасности.
47. Как организовать обучение сотрудников по вопросам информационной безопасности?
48. Какие меры могут быть приняты для снижения риска потери данных?
49. Как осуществляется оценка угроз от внутренних пользователей?
50. Опишите процесс планирования мер по восстановлению после инцидентов безопасности.

3.4 Перечень теоретических вопросов к экзамену

(для оценки знаний)

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.

3.5 Перечень типовых простых практических заданий к экзамену

(для оценки умений)

Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия

1. Определите информационные риски, которые могли способствовать мировому финансовому кризису.

2. Проанализируйте кейс кибертерроризма и предложите меры по снижению таких рисков.

3. Выявите и оцените риски утечки информации в компании, предлагающей электронные отчеты.

4. Изучите существующие государственные регуляции в области информационной безопасности и их влияние на оценку рисков.

5. Подготовьте отчет, включающий оценку рисков как основу для корпоративного управления в конкретной компании.

Раздел 2. Основные этапы и элементы управления рисками и их оценки

6. Опишите основные элементы управления рисками информационной безопасности и приведите примеры.

7. Проведите количественное и качественное определение величины риска для указанного информационного актива.

8. Идентифицируйте ключевые активы организации и оцените их влияние на общие риски информационной безопасности.

9. Сравните подходы к управлению рисками: реактивный и проактивный.

10. Проанализируйте типовые угрозы информационной безопасности и предложите меры их минимизации.

11. Проведите аудит уязвимостей информационной безопасности в небольшом предприятии.

12. Разработайте план обработки рисков для конкретного информационного актива.

13. Определите методы обработки риска и оцените их эффективность для вашего предприятия.

14. Расчет возврата инвестиций в меры по информационной безопасности для конкретного проекта.

Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов

15. Составьте обзор инструментальных средств для управления рисками информационной безопасности.

16. Выберите инструментарий для оценки рисков и объясните выбор.

17. Сравните современные методические подходы к обеспечению защищенности информационных активов.

18. Проанализируйте методику оценки рисков для малого и среднего бизнеса.

Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта

19. Разработайте комплект типовых документов для управления рисками информационной безопасности в предприятии.

20. Подготовьте план внедрения системы управления рисками информационной безопасности.

21. Оцените затраты на обеспечение защищенности информационных активов для крупной компании.

22. Создайте методику оценки информационных рисков для предприятия.

23. Проанализируйте затраты и выгоды от внедрения системы управления информационной безопасностью.

24. Разработайте практические советы по улучшению системы управления рисками информационной безопасности в вашем предприятии.

25. Проведите сравнительный анализ затрат на информационную безопасность в разных секторах экономики.

26. Разработайте проект внедрения системы управления информационными рисками для выбранного предприятия, включая этапы и ключевые действия.

27. Проведите оценку эффективности существующей системы управления информационными рисками на предприятии и предложите улучшения.

28. Разработайте и представьте план обучения сотрудников по вопросам управления информационными рисками.

29. Проведите анализ влияния внешних факторов на систему управления информационными рисками вашего предприятия.

30. Создайте и внедрите систему мониторинга и контроля за реализацией мер по управлению информационными рисками.

3.6 Перечень типовых практических заданий к экзамену

(для оценки навыков и (или) опыта деятельности)

Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия

1. Опишите конкретные информационные риски, способствовавшие мировому финансовому кризису, и предложите способы их управления.

2. Проанализируйте реальный случай кибертерроризма и предложите детальный план мер по его предотвращению.

3. Разработайте процедуру оценки рисков утечки информации в компании, занимающейся электронными отчетами.

4. Исследуйте и представьте примеры государственного регулирования в области

информационной безопасности в разных странах.

5. Составьте подробный отчет об оценке рисков и его интеграции в корпоративное управление конкретной организации.

Раздел 2. Основные этапы и элементы управления рисками и их оценки

6. Создайте схему управления рисками информационной безопасности для малого бизнеса.
7. Проведите количественную и качественную оценку риска для конкретного информационного актива компании.
8. Идентифицируйте и оцените ключевые активы организации, определив их влияние на риски информационной безопасности.
9. Сравните и примените реактивный и проактивный подходы к управлению рисками на практике.
10. Определите и классифицируйте типовые угрозы информационной безопасности для компании, работающей в сфере финансов.
11. Проведите практический аудит уязвимостей информационной безопасности для предприятия среднего размера.
12. Разработайте и реализуйте план обработки рисков для выбранного информационного актива.
13. Проанализируйте и оцените различные методы обработки риска: принятие, уменьшение, передача, избежание.
14. Рассчитайте и обоснуйте возврат инвестиций в меры по информационной безопасности для крупного проекта.

Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов

15. Составьте детальный обзор инструментальных средств управления рисками информационной безопасности.
16. Выберите и обоснуйте использование конкретного инструментария для оценки рисков информационной безопасности.
17. Сравните и примените современные методические подходы к обеспечению защищенности информационных активов на практике.
18. Разработайте методику оценки рисков для малого и среднего бизнеса и протестируйте её.

Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта

19. Разработайте и внедрите комплект типовых документов для управления рисками информационной безопасности в предприятии.
20. Создайте план внедрения системы управления рисками информационной безопасности и оцените его эффективность.
21. Оцените затраты на обеспечение защищенности информационных активов для крупной компании и предложите пути оптимизации.
22. Разработайте и протестируйте методику оценки информационных рисков для конкретного предприятия.
23. Проведите анализ затрат и выгод от внедрения системы управления информационной безопасностью в вашем предприятии.
24. Предложите и реализуйте практические советы по улучшению системы управления рисками информационной безопасности в конкретной компании.
25. Проведите сравнительный анализ затрат на информационную безопасность в различных секторах экономики и предложите рекомендации по их снижению.
26. Разработайте проект внедрения системы управления информационными рисками для выбранного предприятия, включая этапы и ключевые действия.
27. Проведите оценку эффективности существующей системы управления информационными рисками на предприятии и предложите улучшения.
28. Разработайте и представьте план обучения сотрудников по вопросам управления информационными рисками.
29. Проведите анализ влияния внешних факторов на систему управления информационными рисками вашего предприятия.
30. Создайте и внедрите систему мониторинга и контроля за реализацией мер по управлению информационными рисками.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Дискуссия	Дискуссии проводятся во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения дискуссии, доводит до обучающихся тему дискуссии, количество заданий
Конспект	Защита конспектов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему конспектов и требования, предъявляемые к их выполнению и защите
Тестирование (компьютерные технологии)	Тестирование проводится по результатам освоения тем или разделов дисциплины или по окончанию ее изучения во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте, время выполнения. Результаты тестирования видны обучающемуся на компьютере сразу после прохождения теста

Для организации и проведения промежуточной аттестации составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Перечень теоретических вопросов и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

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

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам или в форме компьютерного тестирования.

При проведении промежуточной аттестации в форме собеседования билеты составляются таким образом, чтобы каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; два практических задания: одно из них для оценки умений (выбирается из перечня типовых простых практических заданий к экзамену); другое практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике фондов оценочных средств.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.

Образец экзаменационного билета

<table>
<tr><td>2023-2024 учебный год</td><td>Экзаменационный билет № 1
по дисциплине
«Б1.О.49 «Методология анализа информационных рисков»
Специализация/профиль «Безопасность открытых информационных систем»
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. Определите информационные риски, которые могли способствовать мировому финансовому кризису.
4. Проанализируйте кейс кибертерроризма и предложите меры по снижению таких рисков.
5. Выберите и обоснуйте использование конкретного инструментария для оценки рисков информационной безопасности.
Варианты размеров билета:Билет формата А5 – 148*210мм, Билет формата А4 – 210*297мм</td></tr>
</table>