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.В.ДВ.02.01 Инструментарий анализа информационных рисков

рабочая программа дисциплины

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

Общая трудоемкость в з.е. – 5
Часов по учебному плану (УП) – 180
В том числе в форме практической подготовки (ПП) – 12
(очная)

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

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

Семестр	2	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	102/12	**102/12**
– лекции	34	**34**
– практические (семинарские)	34/12	**34/12**
– лабораторные	34	**34**
Самостоятельная работа	42	**42**
Экзамен	36	**36**
Итого	180/12	**180/12**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

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

Программу составил(и):
к.э.н., доцент, С.П. Серёдкин

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

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

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели дисциплины	
1	раскрытие сущности и значения 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	определить место, роль, специфику системы оценки информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия
2	оценить существующие методические подходы и инструментарий в оценке информационных рисков для выявления возможностей совершенствования данной деятельности
3	изучить особенности организационного направления в деятельности по защите информационных активов и определение их влияния на создание и развитие системы защиты информационных активов хозяйствующего субъекта
4	освоить методические положения и инструментарий в совершенствовании деятельности в сфере оценки информационных рисков хозяйствующих субъектов
5	освоить методические подходы и инструментарий в оценке эффективности деятельности по защите информационных активов предприятия

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Блок/часть ОПОП	Блок 1. Дисциплины / Часть, формируемая участниками образовательных отношений
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.В.ДВ.04.01 Программно-аппаратные средства защиты информации. Дополнительные главы
2	Б2.В.01(П) Производственная - организационно-управленческая практика
3	Б2.В.02(Пд) Производственная - преддипломная практика
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
ПК-2 Способен организовать работы по выявлению недостатков в функционировании системы защиты	ПК-2.1 Анализирует и применяет методы анализа информационных рисков в автоматизированных системах	Знать: - : существующие методические подходы к оценке информационных рисков и основные тенденции развития систем информационной рискозащищенности хозяйствующих субъектов; механизмы оценки последствия от реализации угроз безопасности
		Уметь: - анализировать и оценивать угрозы безопасности при формировании требований пользователя к АС; проводить анализ оценки угроз безопасности информации, с целью повышения эффективности средств и методов ЗИ в АС
		Владеть: - методологией анализа информационных рисков; методикой оценки угроз ИБ; навыками выявлять уязвимости в основных компонентах АС и разрабатывать мероприятия по их устранению; способностью оценивать последствия от реализации угроз безопасности информации в автоматизированной системе

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия.**						

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
1.1	Тема 2. Идентификация активов (описание бизнес-процессов).	7	4	4/2	4	4	ПК-2.1
1.2		7					ПК-2.1
2.0	**Раздел 2. Основные этапы и элементы управления рисками и их оценки.**						
2.1	Тема 3. Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками.	7	4	4	4	4	ПК-2.1
2.2	Тема 4. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	7	4	4/4	4	4	ПК-2.1
2.3	Тема 5. Системный подход к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками, деятельности по управлению рисками (сопровождение и мониторинг механизмов безопасности, пересмотр и переоценка риска, управление документами и записями, корректирующие и превентивные меры, коммуникация рисков). Аутсорсинг процессов управления рисками. Распределение ответственности за управление рисками.	7	6	6	6	6	ПК-2.1
3.0	**Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.**						
3.1	Тема 6. Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками.	7	4	4	4	4	ПК-2.1
3.2	Тема 7. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы.	7	4	4/2	4	6	ПК-2.1
4.0	**Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.**						
4.1	Тема 8. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	7	4	4	4	4	ПК-2.1
4.2	Тема 9. Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность.	7	4	4/4	4	10	ПК-2.1
	Итого часов (без учёта часов на промежуточную аттестацию)		34	34/12	34	42	

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	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
6.1.1.3	Корниенко, А. А. Риск-модели информационной безопасности : учебное пособие / А. А. Корниенко, С. В. Корниенко, А. П. Глухов, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2021. — 79 с. — URL: https://e.lanbook.com/book/191006 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.4	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 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	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

6.1.3 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.В.ДВ.02.01 Инструментарий анализа информационных рисков по направлению подготовки 10.04.01 Информационная безопасность, профиль Безопасность информационных систем и технологий /к.э.н. С.П. Серёдкин; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 11 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47487_1506_2024_1_signed.pdf	Онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»

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

6.3 Программное обеспечение и информационные справочные системы

6.3.1 Базовое программное обеспечение

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

6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License
6.3.2 Специализированное программное обеспечение	
6.3.2.1	MathCAD_student 15.0 Academic_License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01
6.3.2.2	Python 3.9, свободно распространяемое программное обеспечение https://docs.python.org/3/license.html
6.3.2.3	Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/
6.3.2.4	MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01.
6.3.2.5	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01.
6.3.3 Информационные справочные системы	
6.3.3.1	Не предусмотрены
6.4 Правовые и нормативные документы	
6.4.1	Не предусмотрены

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

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

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

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

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией ИрГУПС, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

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

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

ПК-1. Способен организовать работу по выявлению недостатков в функционировании системы защиты и инструментальных средствах программирования

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
7 семестр				
1.0	**Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия**			
1.1	Текущий контроль	Тема 1. Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления.	ПК-1.2	Доклад (устно)
1.2	Текущий контроль	Тема 2. Идентификация активов (описание бизнес-процессов).	ПК-1.2	Доклад (устно) В рамках ПП**: Ситуационная задача (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. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками.	ПК-1.2	Доклад (устно)
2.2	Текущий контроль	Тема 4. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	ПК-1.2	В рамках ПП**: Ситуационная задача (письменно)
2.3	Текущий контроль	Тема 5. Системный подход к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками, деятельности по управлению рисками (сопровождение и мониторинг механизмов безопасности, пересмотр и переоценка риска, управление документами и записями, корректирующие и превентивные меры,	ПК-1.2	Доклад (устно)

		коммуникация рисков). Аутсорсинг процессов управления рисками. Распределение ответственности за управление рисками.		
3.0	**Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов**			
3.1	Текущий контроль	Тема 6. Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками.	ПК-1.2	Доклад (устно)
3.2	Текущий контроль	Тема 7. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы.	ПК-1.2	В рамках ПП**: Ситуационная задача (письменно)
4.0	**Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта**			
4.1	Текущий контроль	Тема 8. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	ПК-1.2	Доклад (устно)
4.2	Текущий контроль	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.	ПК-1.2	В рамках ПП**: Ситуационная задача (письменно)
	Промежуточная аттестация	Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия. Раздел 2. Основные этапы и элементы управления рисками и их оценки. Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.		Зачет (собеседование) Зачет - тестирование (компьютерные технологии)

		Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.		

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.
**ПП – практическая подготовка

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	Ситуационная задача	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности, а также отдельных компетенций (в рамках дисциплины)	Типовое задание для решения ситуационной задачи
2	Доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Зачет	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий к зачету
2	Тест – промежуточная аттестация в форме зачета	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 зачета. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
	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
	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
«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Тест – промежуточная аттестация в форме зачета

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся верно ответил на 70 % и более тестовых заданий при прохождении тестирования
«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Ситуационная задача

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Обучающийся излагает материал логично, грамотно, без ошибок; свободное владеет профессиональной терминологией; умеет высказывать и обосновать свои суждения; дает четкий, полный, правильный ответ на теоретические вопросы; организует связь теории с практикой
«хорошо»		Обучающийся грамотно излагает материал; ориентируется в материале; владеет профессиональной терминологией; осознанно

		применяет теоретические знания для решения кейса, но содержание и форма ответа имеют отдельные неточности. Ответ обучающегося правильный, полный, с незначительными неточностями или недостаточно полный
«удовлетворительно»		Обучающийся излагает материал неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения кейса, не может доказательно обосновать свои суждения; обнаруживается недостаточно глубокое понимание изученного материала
«неудовлетворительно»	«не зачтено»	У обучающегося отсутствуют необходимые теоретические знания; допущены ошибки в определении понятий, искажен их смысл, не решен кейс. В ответе обучающийся проявляется незнание основного материала учебной программы, допускаются грубые ошибки в изложении, не может применять знания для решения кейса

Доклад

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»		Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»		Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	«не зачтено»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль доклада не передана

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

3.1 Типовые контрольные задания для решения ситуационной задачи

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

Ниже приведен образец типовых вариантов заданий для решения ситуационных задач.

Образец типового варианта ситуационной задачи

Тема 2. Идентификация активов (описание бизнес-процессов)

Образец типового варианта ситуационной задачи

Тема 4. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы

Образец типового варианта ситуационной задачи

Тема 7. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе)

для информационной системы; риска реализации по всем угрозам для информационной системы

Образец типового варианта ситуационной задачи

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

3.2 Типовые контрольные темы для написания докладов

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

Ниже приведен образец типовых вариантов тем для написания докладов.

Образец тем докладов

Тема 1. Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм), риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления

1. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов).
2. Государственное регулирование
3. Оценка рисков как основа корпоративного управления»

Образец тем докладов

Тема 2. Идентификация активов (описание бизнес-процессов)

1. Характеристики описания основных бизнес процессов
2. Уровни основных бизнес процессов
3. Классификация бизнес процессов
4. Описание бизнес процесса

Образец тем докладов

Тема 3. Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками

1. Стандарты в области управления рисками информационной безопасности
2. Методика CRAMM
3. Методология COBIT for Risk

Образец тем докладов

Тема 5. Системный подход к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками, деятельности по управлению рисками (сопровождение и мониторинг механизмов безопасности, пересмотр и переоценка риска, управление документами и записями, корректирующие и превентивные меры, коммуникация рисков). Аутсорсинг процессов управления рисками. Распределение ответственности за управление рисками»

1. Системный подход
2. Документации по управлению рисками
3. Аутсорсинг процессов управления рисками

Образец тем докладов

Тема 6. Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками

1. RiskWatch
2. InfoWatch Enterprise Solution (IES)
3. Digital Security Office
4. TA Professional Edition Risk Assessment Tool

Образец тем докладов

Тема 8. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности

1. ISO/IEC 27001
2. ISO/IEC 27005
3. ISO/IEC 31000
4. BS 7799-3

3.3 Типовые контрольные задания для проведения тестирования

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

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ПК-1.2	Тема 1. Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления.	Знание	2 – ОТЗ 8 – ЗТЗ
ПК-1.2	Тема 2. Идентификация активов (описание бизнес-процессов).	Знание	9 – ОТЗ 8 – ЗТЗ
ПК-1.2	Тема 3. Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками.	Знание	9 – ОТЗ 8 – ЗТЗ
		Умение	10 – ОТЗ 10 – ЗТЗ
ПК-1.2	Тема 4. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	Знание	9 – ОТЗ 8 – ЗТЗ
		Умение	10 – ОТЗ 10 – ЗТЗ
ПК-1.2	Тема 5. Системный подход к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками, деятельности по управлению рисками (сопровождение и мониторинг механизмов безопасности, пересмотр и переоценка риска, управление документами и записями, корректирующие и превентивные меры, коммуникация рисков). Аутсорсинг процессов управления рисками. Распределение ответственности за управление рисками.	Знание	9 – ОТЗ 8 – ЗТЗ
ПК-1.2	Тема 6. Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками.	Знание	9 – ОТЗ 8 – ЗТЗ
		Умение	10 – ОТЗ 10 – ЗТЗ
ПК-1.2	Тема 7. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы.	Знание	9 – ОТЗ 8 – ЗТЗ
		Умение	10 – ОТЗ 10 – ЗТЗ

ПК-1.2	Тема 8. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	Знание	9 – ОТЗ 8 – ЗТЗ
		Навык и (или) опыт деятельности/ действие	2 – ОТЗ 6 – ЗТЗ
ПК-1.2	Тема 9. Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность.	Знание	9 – ОТЗ 8 – ЗТЗ
		Умение	10 – ОТЗ 10 – ЗТЗ
		Итого	60

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

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

1. Риск информационной безопасности:

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

   Б) Вероятные потери организации в результате инцидентов;

   В) Возможность минимизации угрозы информационной безопасности.

2. Оценка рисков ИБ, включающая в себя:

   А) Идентификацию риска ИБ и анализ риска ИБ;

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

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

3. Обработка рисков ИБ

   А) Снижение, перенос, уклонение, принятие;

   Б) Страхование;

   В) Хеджирование.

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

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

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

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

5. Каким методами определяется уровень риска информационного актива:

   А) Метод ожидаемых потерь;

   Б) Затратный метод;

   В) Метод аналогий.

6. Технические каналы утечки информации возникают:

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

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

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

7. Основными техническими каналами являются:

   А) Визуально-оптический;

   Б) Акустический;

   В) Электромагнитный.

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

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

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

   В) Должна соответствовать требованиям принципа экономической целесообразности.

9. Категории информационных рисков:

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

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

   В) Риски, вызванные форс-мажорными обстоятельствами.

10. Угрозы безопасности информационным активам это:

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

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

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

11. Риск рассматривается, как поддающаяся измерению вероятность:

А) Причинить негативные последствия;

Б) Создать условия для наступления негативных последствий;

В) Понести убытки или упустить выгоду.

12. Риск определяется:

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

Б) Возможностью реализации угрозы информационной безопасности;

В) Величиной ущерба.

13. Оценка рисков – это:

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

Б) Процедура выявления факторов рисков и оценки их значимости;

В) Выявление характера последствий.

14. Стратегии управления различными классами информационных рисков:

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

Б) Принятие риска;

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

15. Целью анализа рисков является:

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

Б) Проверка уровня защищенности информационной системы;

В) Оценка текущего состояния защищенности информационной системы.

16. Основными источниками угроз информационной безопасности

являются все указанное в списке:

А) Хищение жестких дисков, подключение к сети, инсайдерство

Б) Перехват данных, хищение данных, изменение архитектуры системы

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

17. Виды информационной безопасности:

А) Персональная, корпоративная, государственная

Б) Клиентская, серверная, сетевая

В) Локальная, глобальная, смешанная

18. Цели информационной безопасности – своевременное обнаружение, предупреждение:

А) Несанкционированного доступа, воздействия в сети

Б) Инсайдерства в организации

В) Чрезвычайных ситуаций

19. Основные объекты информационной безопасности:

А) Компьютерные сети, базы данных

Б) Информационные системы, психологическое состояние пользователей

В) Бизнес-ориентированные, коммерческие системы

20. Основными рисками информационной безопасности являются:

А) Искажение, уменьшение объема, перекодировка информации

Б) Техническое вмешательство, выведение из строя оборудования сети

В) Потеря, искажение, утечка информации

21. К основным принципам обеспечения информационной безопасности относится:

А) Экономической эффективности системы безопасности

Б) Многоплатформенной реализации системы

В) Усиления защищенности всех звеньев системы

22. Основными субъектами информационной безопасности являются:

А) руководители, менеджеры, администраторы компаний

Б) органы права, государства, бизнеса

В) сетевые базы данных, фаерволлы

3.4 Перечень теоретических вопросов к зачету

(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)

Тема «Понятие риск. Информационные риски киберпространства».

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

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

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

Тема «Основные элементы управления рисками информационной безопасности».

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

Тема «Система управления информационными рисками».

1. Какие факторы влияют на решение о принятии риска?
2. На основании каких данных определяется вероятность угрозы?
3. Назовите основные источники уязвимостей.
4. Перечислите основные и вспомогательные бизнес-процессы ФГБОУ ВО ИрГУПС.
5. Какие этапы включает в себя оценка риска?
6. Какие параметры могут использоваться для описания бизнес-процессов организации?
7. Какие категории требований безопасности необходимо учитывать при оценке рисков?
8. Как можно определить ценность тех или иных активов?
9. Как связаны между собой оценка рисков и планирование непрерывности бизнеса?

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

1. Раскройте сущность комплексной системы защиты информационных активов предприятий.
2. Опишите особенности система защиты информационных активов хозяйствующего субъекта.
3. Исследуйте особенности организационного направления в деятельности по защите информационных активов предприятия.
4. Охарактеризуйте сущность направления в организационной защите – работе с персоналом, определении его надежности.
5. Как осуществить оценку надежности персонала, как основного источника угроз информационным активам предприятия?
6. Суть методики оценки возможного ущерба при реализации угроз безопасности?
7. Охарактеризуйте сущность направления в организационной защите - информационно-аналитической деятельности по выявлению угроз информационным активам и управлению информационными рисками.
8. Обоснуйте позицию защищенности информационных активов с учетом информационных рисков в деятельности хозяйствующего субъекта.
9. Проведите сравнительный анализ нескольких наиболее известных методик оценки информационных рисков.

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

1. Изложите суть экспертных методов по определению ценности защищаемых

информационных активов.

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

3. Изложите суть эффективности оценки информационных рисков.

3.6 Перечень типовых практических заданий к экзамену

(для оценки навыков и (или) опыта деятельности)

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 (TCO).

Тема «Анализ угроз и уязвимостей»

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

Задание 2. Описать уязвимости информационной безопасности.

Задание 3. Построить модель нарушителя ИБ.

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

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

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

Задание 5. Оцените вероятности угроз.

Тема «Определение величины риска»

Задание 1. Постройте матрицу величины риска.

Задание 2. Откалибруйте шкалу оценки рисков.

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

Тема «Обработка рисков информационной безопасности»

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

Задание 2. Осуществите расчет возврата инвестиций (ROI).

Задание 3. Подготовьте отчет об оценке рисков.

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

Краткая структура отчета об оценке рисков:

1. Введение
2. Основания, общие сведения
3. Цели и задачи
4. Методология и результаты
5. Идентификация активов и требований
6. Оценка активов и последствий
7. Анализ угроз и уязвимостей
8. Вычисление и оценивание рисков
9. Резюме рисков для руководства
9. Описание самых высоких рисков и причин их существования
10. Приложения
11. Реестры активов, требований и рисков

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
Ситуационная задача	Преподаватель не мене, чем за неделю до срока решения ситуационных задач должен довести до сведения обучающихся предлагаемые ситуационные задачи. Решенные ситуационные задачи в назначенный срок сдаются на проверку преподавателю
Доклад	Защита докладов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему докладов и требования, предъявляемые к их выполнению и защите

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. Билеты составлены таким образом, что в каждый из них включал в себя теоретические вопросы и практические задания.

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

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

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

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

Образец экзаменационного билета

ИРГУПС 2021-2022 учебный год	**Экзаменационный билет № 1** **по дисциплине «Инструментарий анализа информационных рисков»** **Специализация/профиль** «Безопасность информационных систем и технологий» 2 **семестр**	Утверждаю: Заведующий кафедрой «ИСиЗИ» ИрГУПС Т.К. Кириллова
1.Оценка возможных последствий реализации угроз безопасности информации. 2.Реагирование на компьютерные инциденты в ходе эксплуатации ИС. 3.Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности ИС. Варианты размеров билета: Билет формата А5 – 148*210мм Билет формата А4 – 210*297мм		