Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.В.ДЭ.05.02
Оценка рисков информационной безопасности
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра бизнес-процессов и экономической безопасности**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 32
самостоятельная работа 39,8
контактная работа во время промежуточной аттестации (ИКР) 0

Виды контроля в семестрах:
зачеты 5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	16	16	16	16
Контактная работа на аттестации	0,2	0,2	0,2	0,2
Итого ауд.	32	32	32	32
Контактная работа	32,2	32,2	32,2	32,2
Сам. работа	39,8	39,8	39,8	39,8
Итого	72	72	72	72

Программу составил(и):

к.ю.н, доцент, Субачев С.Ю.

Рецензент(ы):

кандидат педагогических наук, доцент, доцент кафедры гуманитарных дисциплин Краснодарского филиала ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова», Кирий Е.В.;к.э.н., доцент, директор ООО «СофтСервис-Юг», г. Краснодар, Шупило О.М.

Рабочая программа дисциплины

Оценка рисков информационной безопасности

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:

10.03.01 Информационная безопасность

утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры

Кафедра бизнес-процессов и экономической безопасности

Протокол от 01.11.2023 г. № 4

Зав. кафедрой Маглинова Татьяна Григорьевна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	раскрытие сущности и значения методологии анализа информационных рисков реализации угроз, как основы информационной безопасности и защиты информации, определение теоретических, концептуальных, методических и организационных основ информационной безопасности и защиты ценной для предприятия информации

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

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.ДЭ.05
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Основы информационной безопасности
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Организация и управление службой защиты информации
2.2.2	Системы охраны и инженерной защиты информации
2.2.3	Выполнение и защита выпускной квалификационной работы

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения

ПК-9: Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах

ПК-9.1: Формулирование правил работы персонала со средствами защиты информации

Знать

Уровень 1	Минимальный необходимый уровень знаний формулирования правил работы персонала со средствами защиты информации
Уровень 2	Уровень знаний формулирования правил работы персонала со средствами защиты информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний формулирования правил работы персонала со средствами защиты информации в объёме, соответствующем программе подготовки, без ошибок

ПК-9.2: Распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему

Уметь

Уровень 1	Продемонстрированы основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения распределять обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме

ПК-9.3: Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации

Владеть

Уровень 1	Имеется минимальный набор навыков сопоставления результатов работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки сопоставления результатов работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки сопоставления результатов работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации без

	ошибок и недочётов

ПК-10: Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности	
ПК-10.1: Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний соотношения инцидентов информационной безопасности с характеристиками систем и средств защиты информации
Уровень 2	Уровень знаний соотношения инцидентов информационной безопасности с характеристиками систем и средств защиты информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний соотношения инцидентов информационной безопасности с характеристиками систем и средств защиты информации в объёме, соответствующем программе подготовки, без ошибок
ПК-10.2: Обосновывает необходимость модернизации системы защиты информации автоматизированной системы	
Уметь	
Уровень 1	Продемонстрированы основные умения обосновывать необходимость модернизации системы защиты информации автоматизированной системы, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения обосновывать необходимость модернизации системы защиты информации автоматизированной системы, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения обосновывать необходимость модернизации системы защиты информации автоматизированной системы, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-10.3: Формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности	
Владеть	
Уровень 1	Имеется минимальный набор навыков формулирования правил применения мер защиты информации, направленных на устранение причин возникновения инцидентов информационной безопасности с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулирования правил применения мер защиты информации, направленных на устранение причин возникновения инцидентов информационной безопасности с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулирования правил применения мер защиты информации, направленных на устранение причин возникновения инцидентов информационной безопасности без ошибок и недочётов
ПК-10.4: Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем
Уровень 2	Уровень знаний Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков формулирования правил протоколирования результатов мониторинга безопасности автоматизированных систем с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулирования правил протоколирования результатов мониторинга безопасности автоматизированных систем с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулирования правил протоколирования результатов мониторинга

	безопасности автоматизированных систем без ошибок и недочётов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия					
1.1	Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления. /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
1.2	Идентификация активов (описание бизнес-процессов). /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
1.3	Термины и определения области управления информационными рисками. /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
1.4	Антология кибератак. Наихудшие сценарии кибератак /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
	Раздел 2. Раздел 2. Основные этапы и элементы управления рисками и их оценки.					
2.1	Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками. /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
2.2	Определение ценности активов (критерии оценки ущерба, таблица ценности активов). /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
2.3	Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности. /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	

2.4	Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы. /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
2.5	Базовый опросник для определения степени критичности систем по методу CRAMM. Опросный лист для оценки угроз по методу CRAMM. Опросный лист для оценки уязвимостей по методу CRAMM. /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
2.6	Системный подход к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками, деятельности по управлению рисками (сопровождение и мониторинг механизмов безопасности, пересмотр и переоценка риска, управление документами и записями, корректирующие и превентивные меры, коммуникация рисков). Аутсорсинг процессов управления рисками. распределение ответственности за управление рисками /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
2.7	Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
2.8	Обработка рисков информационной безопасности. Процесс обработки рисков. Способы обработки риска (принятие, уменьшение, передача, избежание риска). Оценка возврата инвестиций в информационную безопасность. План обработки рисков. /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
2.9	Задание контрмер. Расчет риска реализации по всем угрозам для информационной системы после задания контрмер. Эффективность контрмеры. Эффективность комплекса контрмер. Расчет совокупной стоимости владения. Расчет возврата инвестиций /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
2.10	Декларация о применимости механизмов контроля. /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
	Раздел 3. Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.					

3.1	Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками. /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
3.2	Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы. /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
3.3	Программные продукты для управления рисками информационной безопасности. /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
3.4	Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия. /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
3.5	Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001. /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
3.6	Законодательные и нормативные акты Российской Федерации в области защиты информации. /Ср/	5	4,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
3.7	Изучение документов ГТК (защита от несанкционированного доступа к информации). /Ср/	5	5,8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
3.8	BS ISO/IEC27001:2005 (BS 7799-2:2005). Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 779993:2006 ИISO/IEC 27005:2008 /Ср/	5	5,2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
	Раздел 4. Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта					
4.1	Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности. /Лек/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	

4.2	Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность. /Пр/	5	2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	
	Раздел 5. Промежуточная аттестация					
5.1	Зачет /КА/	5	0,2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-10.1 ПК-10.2 ПК-10.3 ПК-10.4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

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.

5.2. Темы письменных работ

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.

5.3. Фонд оценочных средств

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.

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых верный(ые). Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Вавилина А. В., Калашников И. Б.	Экономическая безопасность и инновационная политика: Учебное пособие	Москва: КноРус, 2020, URL: https://book.ru/book/935903
Л1.2	Дергачев К. В., Титарев Д. В.	Защита информации: лабораторный практикум: Учебное пособие	Москва: Русайнс, 2021, URL: https://book.ru/book/940250
Л1.3	Гуреева М. А.	Экономическая безопасность: Учебник	Москва: КноРус, 2020, URL: https://book.ru/book/938284
Л1.4	Вавилина А. В., Мосейкин Ю. Н., Калашников И. Б.	Права собственности: экономическая теория и экономическая безопасность: Учебное пособие	Москва: КноРус, 2021, URL: https://book.ru/book/941490
Л1.5	Жук А.П., Жук Е.П.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021, URL: http://znanium.com/catalog/document?id=367588

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Москвитин Г. И.	Комплексная защита информации в организации: Монография	Москва: Русайнс, 2020, URL: https://book.ru/book/934814
Л2.2	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: http://znanium.com/catalog/document?id=366835
Л2.3	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2022, URL: https://znanium.com/catalog/document?id=393765

6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL

6.3.2. Перечень профессиональных баз данных и информационных справочных систем

6.3.2.1	Консультант Плюс http://www.consultant.ru
6.3.2.2	Кодекс – Профессиональные справочные системы https://kodeks.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
230	Кабинет гуманитарных и социально-экономических дисциплин	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice	Парта ученическая со скамьей (2-местная) – 14 шт., рабочее место преподавателя– 1 шт., доска учебная - 1 шт., персональный компьютер - 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., учебно-методическая литература, учебно-наглядные методические пособия, соответствующее программное обеспечение
121	Компьютерный класс	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее

		LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate ПО ЛИНКО v8.2 демо-версия Klite Mega Codec Pack Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	программное обеспечение
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.
Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.
Учебный материал по дисциплине «Оценка рисков информационной безопасности», разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ. Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только

знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).
Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.
Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.
Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Оценка рисков информационной безопасности».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.
Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями