МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«26» сентября 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
наименование дисциплины

Специальность
10.05.03 Информационная безопасность автоматизированных систем
шифр *наименование специальности*

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
наименование специализации

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	9

Магнитогорск
2018 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«07» сентября 2018 г., протокол № 1.

Зав. кафедрой _____ / И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«26» сентября 2018 г., протокол № 1.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)
_____ / И.И. Баранкова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)
_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
2.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
3.	7	Переработка фонда оценочных средств	№ 1 от 04.09.2020	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 04.09.2020	

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины (модуля) «Анализ рисков информационной безопасности» являются: выявление источников и способов реализации угроз информационной безопасности, фиксация параметров безопасности и анализа безопасности АС, изучение основных понятий и принципов анализа и оценки рисков информационной безопасности.

2 Место дисциплины (модуля) в структуре образовательной программы подготовки специалиста

Дисциплина «Анализ рисков информационной безопасности» входит в вариативную часть блока 1 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин: Моделирование угроз информационной безопасности, Организационное и правовое обеспечение информационной безопасности, Разработка и эксплуатация защищенных автоматизированных систем, Методы выявления нарушений информационной безопасности, аттестация АИС.

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для научно-исследовательской работы, производственной преддипломной практики, подготовки к ГИА и выполнения ВКР.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Анализ рисков информационной безопасности» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	
Знать	– методологию анализа рисков информационной безопасности – методики определения информационно-технологических ресурсов, подлежащих защите – способы применения анализа рисков в информационной безопасности при работе над междисциплинарными проектами – перечень информационно-технологических ресурсов, подлежащих защите способы применения анализа рисков в информационной безопасности при работе над инновационными проектами
Уметь	– применять терминологию анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами – выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите
Владеть	– терминологией, используемой при анализе особенностей деятельности организации и использования в ней автоматизированных систем с целью определения

Структурный элемент компетенции	Планируемые результаты обучения
	информационно-технологических ресурсов, подлежащих защите – навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите
ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	
Знать	– о политиках безопасности и мерах защиты в распределённых приложениях – способы обеспечения информационной безопасности систем организационного управления – Методы и средства определения технологической безопасности функционирования распределенной информационной системы – методы и процедуры выявления угроз информационной безопасности в защищённых распределённых приложениях
Уметь	– формулировать основные требования к методам и средствам защиты информации в защищённых распределённых приложениях – Оценивать информационные риски в автоматизированных системах – выполнять анализ рисков информационной безопасности в распределенных информационных системах – Анализировать и оценивать угрозы информационной безопасности объекта выполнять анализ рисков информационной безопасности в распределенных информационных системах
Владеть	– методиками проведения анализа рисков информационной безопасности распределенных информационных систем – Методами оценки информационных рисков – Навыками разработки политики информационной безопасности автоматизированных систем

4 Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:
- контактная работа – 86,8 акад. часов:
- аудиторная – 85 акад. часов;
- внеаудиторная – 1,8 акад. часов
- самостоятельная работа – 57,2 акад. часов;
- форма промежуточного контроля - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	занятиялаборат.	практич. занятия				
Тема 1. Оценочные стандарты в информационной безопасности. Роль стандартов информационной безопасности. «Критерии определения безопасности компьютерных систем» как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.	9	6		10/2И	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме.	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	**ПСК-7.2 з ПК-5 з**
Тема 2. Методика оценки рисков информационной безопасности предприятия. Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей.		6		10/4И	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных	**ПСК-7.2 зу ПК-5 зу**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	занятиялаборат.	практич. занятия				
						библиотеками. Поиск дополнительной информации по заданной теме	заданий	
Тема 3. Методика оценки рисков информационной организации. Метод оценки рисков на основе модели информационных потоков. Расчет рисков по угрозе конфиденциальность.	9	6		7/4И	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	**ПСК-7.2 зув** **ПК-5 зув**
Тема 4. Методики и технологии управления рисками. Качественные методики управления рисками. Количественные методики управления рисками. Метод CRAMM.	9	6		7/4И	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	**ПСК-7.2 зу** **ПК-5 зу**
Тема 5. Разработка корпоративной методики анализа рисков. Постановка задачи. Методы оценивания информационных рисков. Табличные	9	6		7/4И	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы.	– устный опрос (собеседование); – контрольные работы; – семинарские занятия;	**ПСК-7.2 зув** **ПК-5 зув**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	занятиялаборат.	практич. занятия				
методы оценки рисков. Оценка рисков по двум факторам. Разделение рисков на приемлемые и неприемлемые. Оценка рисков по трем факторам. Методика анализа рисков Microsoft.						Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– проверка индивидуальных заданий	
Тема 6 Современные методы и средства анализа и управление рисками информационных систем. Методика FRAP. Методика OCTAVE. Методика RiskWatch.	9	4		10/4И	7,2	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	**ПСК-7.2 зу ПК-5 зу**
Итого за семестр	**9**	**34**		**51/22И**	**57,2**		**Промежуточная аттестация (зачет)**	
Итого по дисциплине	**9**	**34**		**51/22И**	**57,2**		**Промежуточная аттестация (зачет)**	

И – в том числе, часы, отведенные на работу в интерактивной форме.

5 Образовательные и информационные технологии

Согласно п. 34 Порядка организации и осуществления деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом МОиН РФ от 05.04.2017 г. № 301) **при проведении учебных занятий организация обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств** (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

1. **Традиционные образовательные технологии** ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к студенту (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность студента носит в таких условиях, как правило, репродуктивный характер.

Формы учебных занятий с использованием традиционных технологий:

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Семинар – беседа преподавателя и студентов, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы.

Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. **Технологии проблемного обучения** – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности студентов.

Формы учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала.

Лекция «вдвоем» (бинарная лекция) – изложение материала в форме диалогического общения двух преподавателей (например, реконструкция диалога представителей различных научных школ, «ученого» и «практика» и т.п.).

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от студента применения как научно-теоретических знаний, так и практических навыков.

Практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации.

3. **Игровые технологии** – организация образовательного процесса, основанная на реконструкции моделей поведения в рамках предложенных сценарных условий.

Формы учебных занятий с использованием игровых технологий:

Учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.

Деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Ролевая игра – имитация или реконструкция моделей ролевого поведения в предложенных сценарных условиях.

4. **Технологии проектного обучения** – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы студентов, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлксию.

Основные типы проектов:

Исследовательский проект – структура приближена к формату научного исследования (доказательство актуальности темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, выдвижение гипотезы, обобщение результатов, выводы, обозначение новых проблем).

Творческий проект, как правило, не имеет детально проработанной структуры; учебно-познавательная деятельность студентов осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия и т.п.).

Информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

5. **Интерактивные технологии** – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды.

Формы учебных занятий с использованием специализированных интерактивных технологий:

Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-прессконференция.

Семинар-дискуссия – коллективное обсуждение какого-либо спорного вопроса, проблемы, выявление мнений в группе (межгрупповой диалог, дискуссия как спор-диалог).

6. **Информационно-коммуникационные образовательные технологии** – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией.

Формы учебных занятий с использованием информационно-коммуникационных технологий:

Лекция-визуализация – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).

Практическое занятие в форме презентации – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Перечень тем для подготовки к практическим занятиям:

Тема 1. Основные понятия информационной безопасности

– Понятие информационной безопасности.

– Основные составляющие информационной безопасности.

– Управление информационной безопасностью.

– Важность и сложность проблемы информационной безопасности.

Тема 2. Оценочные стандарты в информационной безопасности.

– Роль стандартов информационной безопасности.

– «Критерии определения безопасности компьютерных систем» как оценочный стандарт.

– Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.

Тема 3. Стандарты управления информационной безопасностью.

–Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799.

–Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования".

–Сертификация СУИБ на соответствие ISO 27001.

Тема 4. Создание СУИБ на предприятии.

–Этапы разработки и внедрения системы управления ИБ.

–Содержание этапов разработки и внедрения системы управления ИБ.

Тема 5. Методика оценки рисков информационной безопасности предприятия.

–Управление рисками. Основные понятия.

–Метод оценки рисков на основе модели угроз и уязвимостей.

Тема 6. Методика оценки рисков информационной организации.

– Метод оценки рисков на основе модели информационных потоков.

– Расчет рисков по угрозе конфиденциальность.

Тема 7. Методики и технологии управления рисками.

– Качественные методики управления рисками.

– Количественные методики управления рисками. Метод CRAMM.

Тема 8. Разработка корпоративной методики анализа рисков.

– Методы оценивания информационных рисков.

– Табличные методы оценки рисков.

– Оценка рисков по двум факторам.

– Разделение рисков на приемлемые и неприемлемые.

– Оценка рисков по трем факторам.

– Методика анализа рисков Microsoft.

Тема 9 Современные методы и средства анализа и управление рисками информационных систем.

– Методика FRAP.

– Методика OCTAVE.

– Методика RiskWatch.

Перечень контрольных вопросов по терминологии:

Угроза (Threat)

Уязвимость (Vulnerability)

- *Анализ рисков.*

Базовый уровень безопасности .

Базовый (Baseline) анализ рисков .

Полный (Full) анализ рисков.

Риск нарушения ИБ (Security Risk).
Оценка рисков (Risk Assessment).
Управление рисками (Risk Management).
Система управления ИБ (Information Security Management System).
Класс рисков.

Терминология COBIT

- *Риски*

Типы рисков.
Приемлемый уровень риска
Стандарт управления рисками.
Матрица ИТ рисков.

- *Руководство рисками*

Владелец процессов оценки рисков.
План работ по снижению рисков.
Политики и процедуры.
Обновление величин рисков.
Глобальный и системный уровни оценки ИТ- рисков.
Резюме для руководителя.
Стратегия управления ИТ

- *Идентификация*

Определение компонентов риска.
Области рисков.
Обновление матрицы рисков.
Меры оценки
Количественная оценка.
Качественная оценка.

- *Способы управления*

Независимое мнение.
Возврат инвестиций.
Баланс способов управления
Управление конфликтами.

- *Мониторинг*

Мониторинг используемых способов управления.
Процедура реагирования на инциденты .
Согласование плана работ по снижению рисков .

7 Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы		
Знать	– методологию анализа рисков информационной безопасности – методики определения информационно-технологических ресурсов, подлежащих защите – способы применения анализа рисков в информационной безопасности при работе над междисциплинарными проектами – перечень информационно-технологических ресурсов, подлежащих защите способы применения анализа рисков в информационной безопасности при работе над инновационными проектами	1. Назвать угрозы информационной безопасности в информационных системах. 2. Перечислить оценочные стандарты в информационной безопасности. 3. Описать «Оранжевую книгу» как оценочный стандарт. 4. Международный стандарт ISO/IEC 15408. Описать критерии оценки безопасности информационных систем. 5. Перечислить стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. 6. Международный стандарт ISO/IEC 27001:2005 Назвать требования к системам управления информационной безопасностью. 7. Сертификация СУИБ на соответствие ISO 27001. 8. Методика оценки рисков информационной безопасности компании. 9. Управление рисками. Перечислить основные понятия. 10. Метод оценки рисков на основе модели угроз и уязвимостей. 11. Расчет рисков по угрозе информационной безопасности. 12. Метод оценки рисков на основе модели информационных потоков. 13. Методики и технологии управления рисками. Качественные методики управления рисками. Количественные методики управления рисками. Метод CRAMM. 14. Разработка корпоративной методики анализа рисков. 15. Современные методы и средства анализа и управление рисками информационных систем компаний. 16. Обоснование необходимости инвестиций в информационную безопасность

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		компании.
Уметь	– применять терминологию анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами – выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	Провести расчеты оценки рисков информационной безопасности компании по методу оценки рисков на основе частной модели угроз.
Владеть	– терминологией, используемой при анализе особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите – навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	***Задание:*** Для заданного предприятия определить: • информационные активы компании; • ценность активов; • какие угрозы могут повлиять на информационные активы; • с помощью каких механизмов можно защитить ключевые активы; • уровень риска и предполагаемых потерь. провести оценку рисков ИБ (по выдранной методике): • инвентаризацию информационных активов и их стоимости; • определение методологии, необходимой для проведения оценки рисков и ее применение в конкретной компании; • анализ возможных угроз и уязвимостей; • определение мер, направленных на осуществление ИБ; • создать матрицу рисков; • осуществить количественную и качественную оценку рисков; • подготовить отчет о выполненной работе по оценке рисков;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		• подготовить плана оптимизации рисков. Представить результат работы: • подготовить карту информационных активов фирмы; • составить карты уязвимостей и угроз; • подготовить отчет о результатах оценки рисков; • подготовить план по обработке рисков.
ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах		
Знать	– о политиках безопасности и мерах защиты в распределённых приложениях – способы обеспечения информационной безопасности систем организационного управления – Методы и средства определения технологической безопасности функционирования распределенной информационной системы – методы и процедуры выявления угроз информационной безопасности в защищённых распределённых приложениях	1. Назвать угрозы информационной безопасности в информационных системах. 2. Перечислить оценочные стандарты в информационной безопасности. 3. Описать «Оранжевую книгу» как оценочный стандарт. 4. Международный стандарт ISO/IEC 15408. Описать критерии оценки безопасности информационных систем. 5. Перечислить стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. 6. Международный стандарт ISO/IEC 27001:2005 Назвать требования к системам управления информационной безопасностью. 7. Сертификация СУИБ на соответствие ISO 27001. 8. Методика оценки рисков информационной безопасности компании. 9. Управление рисками. Перечислить основные понятия. 10. Метод оценки рисков на основе модели угроз и уязвимостей. 11. Расчет рисков по угрозе информационной безопасности. 12. Метод оценки рисков на основе модели информационных потоков. 13. Методики и технологии управления рисками. Качественные методики управления рисками. Количественные методики управления рисками. Метод CRAMM. 14. Разработка корпоративной методики анализа рисков. 15. Современные методы и средства анализа и управление рисками информационных систем компаний.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		16. Обоснование необходимости инвестиций в информационную безопасность компании.
Уметь	– формулировать основные требования к методам и средствам защиты информации в защищённых распределённых приложениях – Оценивать информационные риски в автоматизированных системах – выполнять анализ рисков информационной безопасности в распределенных информационных системах – Анализировать и оценивать угрозы информационной безопасности объекта выполнять анализ рисков информационной безопасности в распределенных информационных системах	Провести расчеты оценки рисков информационной безопасности компании по оценки рисков на основе модели информационных потоков.
Владеть	– методиками проведения анализа рисков информационной безопасности распределенных информационных систем – Методами оценки информационных рисков – Навыками разработки политики информационной безопасности автоматизированных систем	***Задание*** Для заданного предприятия определить: • информационные активы компании; • ценность активов; • какие угрозы могут повлиять на информационные активы; • с помощью каких механизмов можно защитить ключевые активы; • уровень риска и предполагаемых потерь. провести оценку рисков ИБ (по выдранной методике): • инвентаризацию информационных активов и их стоимости; • определение методологии, необходимой для проведения оценки рисков и ее применение в конкретной компании;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		• анализ возможных угроз и уязвимостей; • определение мер, направленных на осуществление ИБ; • создать матрицу рисков; • осуществить количественную и качественную оценку рисков; • подготовить отчет о выполненной работе по оценке рисков; • подготовить плана оптимизации рисков. Представить результат работы: • подготовить карту информационных активов фирмы; • составить карты уязвимостей и угроз; • подготовить отчет о результатах оценки рисков; • подготовить план по обработке рисков.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

– на оценку «**зачтено**» – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на оценку «**не зачтено**» – обучающийся не может показать знания на уровне воспроизведения и объяснения информации.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: http://znanium.com/bookread2.php?book=997108
2. Управление информационными рисками. Экономически оправданная безопасность: Пособие / Петренко С.А., Симонов С.В., - 2-е изд., (эл.) - М.:ДМК Пресс, 2018. - 396 с. http://znanium.com/bookread2.php?book=983162
3. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.

б) Дополнительная литература:

1. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов Авторы: Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Москва: Горячая Линия–Телеком, 2013 г. , 166 с. НРежим достураhttp://ibooks.ru/reading.php?productid=334014
2. Козлова Е. А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации // Молодой ученый. — 2013. — №5. — С. 154-161. — URL https://moluch.ru/archive/52/6967/ .
3. Основы управления информационной безопасностью. Учебное пособие для вузов Авторы: Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Москва: Горячая Линия–Телеком, 2013 г. , 244 с. http://ibooks.ru/reading.php?productid=334010
4. Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с.– Режим доступа: http://znanium.com/bookread.php?book=463037 .–Заглавие с экрана.
5. Астахов, А.М. Искусство управления информационными рисками [Текст]/ А. М. Астахов. – М.: Изд. ДМК Пресс, 2010. – 312 с. – ISBN 978-5-94074-574-7.
6. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.- (Высшее образование). –Режим доступа: http://znanium.com/bookread.php?book=402686 .–Заглавие с экрана.–ISBN 978-5-8199-0411-4.
7. Петренко, С.А., Политики информационной безопасности [Текст]/ С.А. Петренко, В.А. Курбатов. – М.: Компания АйТи, 2010. – 400 с.–ISBN 2-5-98453-024-4.

в) Программное обеспечение и Интернет-ресурсы:

1. ЭБС "КОНСУЛЬТАНТ СТУДЕНТА" http://www.studentlibrary.ru/catalogue/switch_kit/x2016-034.html
2. Банк данных угроз безопасности информации [Электронный ресурс] – Режим доступа: https://bdu.fstec.ru .– Загл. с экрана. Яз. рус.
3. 1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.
4. 2. Журнал «Безопасность информационных технологий» : периодич. интернет-изд. URL: http://www.pvti.ru/articles_18.htm – Загл. с экрана. Яз. рус.
5. 3. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL:

http://cyberrus.com/ – Загл. с экрана. Яз. рус.
6. 4. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД".http://www.osp.ru/os/– Загл. с экрана. Яз. рус.
7. 5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru , свободный.– Загл. с экрана. Яз. рус.
8. 6. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru . Яз. рус.
9. 7. Безопасник [Электронный ресурс] – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.
10. 8. Компьютерра: все новости про компьютеры, железо, новые технологии, информационные технологии [Электронный ресурс]. – Периодическое электронное Интернет-издание – Режим доступа: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.
11. 9. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/ .– Загл. с экрана. Яз. рус.

9 Материально-техническое обеспечение дисциплины

Тип и название аудитории	Оснащение аудитории
Лекционная аудитория (ауд. 2124, ауд. 226, 309а, ауд. 365, ауд. 388 и т.д.)	Мультимедийные средства хранения, передачи и представления информации
Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.)	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.
Аудитория для самостоятельной работы читальные залы библиотеки, ауд 132а	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.