

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Емельянов Сергей Геннадьевич
Должность: ректор
Дата подписания: 17.12.2021 20:11:40
Уникальный программный ключ:
9ba7d3e34c012eba476ffd2d064cf2781953be730df2374d16f3c0ce536f0fc6

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет



УТВЕРЖДАЮ:

Проректор по научной работе
(наименование должности полностью)

О.Г. Добросердов

(подпись, инициалы, фамилия)

« 28 » 06 20 16 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы анализа рисков нарушения информационной безопасности (наименование дисциплины)

направление подготовки 10.06.01
шифр согласно ФГОС ВО

Информационная безопасность
наименование направления подготовки

Методы и системы защиты информации, информационная безопасность
наименование профиля (специализация подготовки)

квалификация (степень) выпускника: Исследователь. Преподаватель-исследователь

форма обучения очная
(очная, заочная)

Курс – 2016

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (уровень подготовки кадров высшего образования) направления подготовки 10.06.01 «Информационная безопасность», на основании учебного плана профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 11 «27» 06 2016 г.

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения аспирантов по направлению подготовки 10.06.01 «Информационная безопасность», профиля (специализации) «Методы и системы защиты информации, информационная безопасность» на заседании кафедры информационной безопасности, протокол № 1 от «30» 08 2016 г.

Зав. кафедрой _____ М.О. Таныгин

Разработчик программы _____ Ю.А. Халин

Согласовано:

Директор научной библиотеки _____ В.Г. Макаровская

Начальник отдела аспирантуры и докторантуры _____ О.Ю. Прусова

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 5 «30» 08 2017 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол 1 от 28.08.2017

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 8 «26» 03 2018 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол 12 от 28.06.2018.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 9 «24» 06 2019 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол 11 от 27.06.2019.

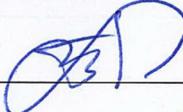
Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 11 «29» 06 2020г. на заседании кафедры информационной безопасности.

Зав.
кафедрой _____

 / протокол N 1 от 31.08.2020

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 8 «31» 05 2021г. на заседании кафедры информационной безопасности.

Зав.
кафедрой _____

 / протокол N 11 от 28.06.2021

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № __ «__» _____ 20__ г. на заседании кафедры информационной безопасности.

Зав.
кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № __ «__» _____ 20__ г. на заседании кафедры информационной безопасности.

Зав.
кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № __ «__» _____ 20__ г. на заседании кафедры информационной безопасности.

Зав.
кафедрой _____

1 Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения ОП

1.1 Цель преподавания дисциплины

Целью преподавания дисциплины является ознакомление студентов с природой и содержанием понятий «неопределенность» и «риск», основными принципами и методами оценивания риска, принятия решений при неопределенности, моделирования систем защиты информации в условиях неопределенности и риска.

1.2 Задачи изучения дисциплины

Задачами освоения дисциплины являются:

- раскрыть различные аспекты усиления неопределенности и полезности риска;
- выделить критерии классификации рисков и охарактеризовать виды рисков в соответствии с выделенными критериями;
- ознакомить с теоретическими основами исследования рисков;
- охарактеризовать традиционные и современные методы исследования рисков, методы количественной оценки рисков;
- ознакомить с основными аксиомами и элементами современной теорией рисков и существующими концепциями риска;
- представить порядок проведения исследования рисков;
- охарактеризовать ценность информации в рискованных ситуациях;
- охарактеризовать критерии выбора в рискованных ситуациях;
- изучить методы моделирования рискованных ситуаций и обоснования решений;
- получение практических навыков идентификации рисков, сопровождающих те или иные виды деятельности в сфере информационной безопасности, связанных с той или иной ситуацией, формализации рискованных ситуаций, выбора методов оценки рисков и принятия решений.

1.3 Компетенции, формируемые в результате освоения дисциплины

У обучающихся формируются следующие **компетенции**:

- способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);
- способностью обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности(ОПК-3);

- способностью к решению научных и технических проблем разработки новых и совершенствования имеющихся методов и средств защиты информации и обеспечения информационной безопасности объектов (ПК-1);

- способностью исследовать угрозы нарушения информационной безопасности и совершенствовать методы, способы и средства защиты информации в процессе ее сбора, хранения и обработки (ПК-2)

- способностью к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1)

2 Место дисциплины в структуре образовательной программы

Дисциплина «Методы анализа рисков нарушения информационной безопасности» (Б1.В.ОД.5) находится в базовом блоке УП, изучается на 2 курсе, в 3 семестре.

3 Содержание и объем дисциплины»

3.1 Содержание дисциплины и лекционных занятий

Общая трудоемкость (объем) дисциплины составляет 2 зачетных единицы (з.е.), 72 часа.

Таблица 3.1 –Объём дисциплины по видам учебных занятий

Объём дисциплины	Всего, часов
Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	
в том числе:	36,1
лекции	18
лабораторные занятия	не предусмотрено
практические занятия	18
экзамен	не предусмотрено
зачет	0,1
Аудиторная работа (всего):	36
в том числе:	
лекции	18
лабораторные занятия	не предусмотрено
практические занятия	18
Самостоятельная работа обучающихся (всего)	36
Контроль/экз (подготовка к экзамену)	не предусмотрено

Таблица 3.2 – Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел(тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра)	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Введение. Базовые вопросы управления ИБ.	1, 2 часа	0	1	У-1 У-2	КО 1 неделя	ОПК1 ОПК-3 ПК-1 ПК-2 УК-1
2	Оценочные стандарты в информационной безопасности	2, 2 часа	0	2	У-1 У-2	КО 2 неделя	ОПК1 ОПК-3 ПК-1 ПК-2 УК-1
3	Стандарты управления информационной безопасностью	3, 2 часа	0	3	У-1 У-2	К 3 неделя	ОПК1 ОПК-3 ПК-1 ПК-2 УК-1
4	Создание СУИБ на предприятии	4, 2 часа	0	4	У-1 У-2	КО 4 неделя	ОПК1 ОПК-3 ПК-1 ПК-2 УК-1
5	Анализ рисков информационной безопасности компании	5, 2 часа	0	5	У-1 У-2	КО 5 неделя	ОПК1 ОПК-3 ПК-1 ПК-2 УК-1
6	Методика оценки рисков информационной безопасности компании	6, 2 часа	0	6	У-1 У-2 У-3	КО 6 неделя	ОПК1 ОПК-3 ПК-1 ПК-2 УК-1
7	Методики и технологии управления рисками	7, 2 часа	0	7	У-1 У-2	К 7 неделя	ОПК1 ОПК-3 ПК-1 ПК-2 УК-1
8	Разработка корпоративной методики анализа рисков	8, 2 часа	0	8	У-1 У-2	КО 8 неделя	ОПК1 ОПК-3 ПК-1 ПК-2 УК-1
9	Современные методы и средства анализа и управление рисками информационных систем компаний	9, 2 часа	0	9	У-1 У-2	КО 9 неделя	ОПК1 ОПК-3 ПК-1 ПК-2 УК-1
10	ИТОГО	18				3	

Таблица 3.3 – Краткое содержание лекционного курса

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Тема 1. Введение. Базовые вопросы управления ИБ.	Наука управления. Понятие СУИБ. Стандартизация в области построения систем управления.
2	Тема 2. Оценочные стандарты в информационной безопасности	Роль стандартов ИБ. «Оранжевая книга» как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.
3	Тема 3. Стандарты управления информационной безопасностью	Стандарты управления информационной безопасностью. BS 7799 и ISO/IEC 17799. Их основные положения. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасностью. Требования". Сертификация СУИБ на соответствие ISO 27001.
4	Тема 4. Создание СУИБ на предприятии	Этапы создания системы управления ИБ. Категорирование активов компании. Оценка защищенности информационной системы компании. Оценка информационных рисков.
5	Тема 5. Анализ рисков информационной безопасности компании	Управление рисками. Понятие информационного риска. Информационные риски и защита информации. Постановка задачи анализа информационных рисков.
6	Тема 6. Методика оценки рисков информационной безопасности компании	Метод оценки рисков на основе модели информационных потоков. Описание архитектуры ИС. Расчет рисков по угрозе конфиденциальность.
7	Тема 7. Методики и технологии управления рисками	Качественные методики управления рисками Количественные методики управления рисками. Метод CRAMM
8	Тема 8. Разработка корпоративной методики анализа рисков	Методы оценивания информационных рисков. Табличные методы оценки рисков. Методика анализа рисков Microsoft
9	Тема 9. Современные методы и средства анализа и управление рисками информационных систем компаний	Обоснование необходимости инвестиций в информационную безопасность компании Методика FRAP Методика OCTAVE (октэйв) Методика RiskWatch (риск вэтч)

3.2 Лабораторные работы и (или) практические занятия

3.2.2 Практические занятия

Таблица 3.4 – Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1	Методы теории вероятностей и статистические методы исследования и оценки рисков	2
2	Анализ модели угроз ИБ и уязвимостей	2
3	Анализ модели информационных потоков.	2
4	Оценка тяжести последствий нарушения режима ИБ	2
5	Измерения ценности информации	2
6	Методы построения функций принадлежности требований к СЗИ заданному уровню качества	2
7	Основные элементы управления рисками информационных систем. Система управления информационными рисками	2
8	Оценка рисков по двум факторам. Оценка рисков по трем факторам.	2
9	Управление инцидентами ИБ	2
Итого		18

3.3 Самостоятельная работа аспирантов (СРС)

Таблица 3.5 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Основные стратегии управления рисками. Подготовка <i>доклада с презентацией</i> и выступление с ним на практическом занятии	2 - 3 неделя	6
2	Анализ инструментальных средств оценки рисков утечки информации в компьютерной сети предприятия. Подготовка <i>доклада с презентацией</i> и выступление с ним на практическом занятии	4 - 5 неделя	6
3	Оценка уровня защищенности информационных процессов. Подготовка <i>доклада с презентацией</i> и выступление с ним на круглом столе	6 - 7 неделя	8
4	Измерения ценности информации. Подготовка <i>доклада с презентацией</i> и выступление с ним на круглом столе	8 - 16 неделя	8
5	Основные элементы управления рисками информационных систем. Система управления информационными рисками. Подготовка <i>доклада с презентацией</i> и выступление с ним на круглом столе	17 - 18 неделя	8
Итого			36

Общие рекомендации аспирантам изложены в Методических указаниях к выполнению самостоятельной работы.

4 Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

Аспиранты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки:

– методических рекомендаций, пособий по организации самостоятельной

– работы студентов;

– тем рефератов;

– вопросов к зачету;

– методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

– удовлетворение потребности в тиражировании научной, учебной и методической литературы.

5 Образовательные технологии

В соответствии с требованиями Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.06.01 – «Информационная безопасность», утвержденного Министерством

образования и науки Российской Федерации приказом № 301 от 05.04.2017г., реализация компетентного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков аспирантов. В рамках дисциплины предусмотрены встречи с экспертами и специалистами по информационной системам.

Таблица 5.1 – Образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Образовательные технологии	Объем, час.
1	2	3	4
1	Методика оценки рисков информационной безопасности компании	лекция с элементами проблемного изложения	2
2	Методики и технологии управления рисками	технологии эвристического обучения	2
3	Разработка корпоративной методики анализа рисков	технологии коллективной мыслительной деятельности	2
4	Современные методы и средства анализа и управление рисками информационных систем компаний	технологии развития критического мышления	2
Итого:			8

6 Фонд оценочных средств для проведения промежуточной аттестации

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 6.1 Этапы формирования компетенции

Код компетенции, содержание компетенции	Дисциплины (модули) при изучении которых формируется данная компетенция
1	2
ОПК-1 способностью самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных	Б1.В.ОД.4 Методология научных исследований Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.1.2 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.2 Научно-исследовательская практика

технологий	<p>Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук</p> <p>Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)</p>
<p>ОПК-3</p> <p>способностью обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности</p>	<p>Б1.В.ОД.4 Методология научных исследований</p> <p>Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности</p> <p>Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность</p> <p>Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации</p> <p>Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации</p> <p>Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена</p> <p>Б2.2 Научно-исследовательская практика</p> <p>Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук</p> <p>Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)</p>
<p>ПК-1</p> <p>способностью к решению научных и технических проблем разработки новых и совершенствования имеющихся методов и средств защиты информации и обеспечения информационной безопасности объектов</p>	<p>Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности</p> <p>Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность</p> <p>Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел как средство реализации асимметричного шифрования</p> <p>Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена</p> <p>Б2.2 Научно-исследовательская практика</p> <p>Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук</p> <p>Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)</p>
<p>ПК-2</p> <p>способностью исследовать угрозы нарушения информационной безопасности и совершенствовать методы, способы и средства защиты информации в процессе ее сбора, хранения и обработки</p>	<p>Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности</p> <p>Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность</p> <p>Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации</p> <p>Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена</p> <p>Б2.2 Научно-исследовательская практика</p> <p>Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук</p> <p>Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)</p>
<p>УК-1</p> <p>способность к критическому анализу и оценке современных научных</p>	<p>Б1.Б.1 История и философия науки</p> <p>Б1.В.ОД.1 Методология науки и образовательной деятельности</p> <p>Б1.В.ОД.4 Методология научных исследований</p> <p>Б1.В.ОД.5 Методы анализа рисков нарушения информационной</p>

<p>достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях</p>	<p>безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.2 Технология идентификации и аутентификации пользователей и субъектов информационных процессов Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел как средство реализации асимметричного шифрования Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.1 Педагогическая практика Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)</p>
--	---

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

- раскрыть различные аспекты усиления неопределенности и полезности риска;
- выделить критерии классификации рисков и охарактеризовать виды рисков в соответствии с выделенными критериями;
- ознакомить с теоретическими основами исследования рисков;
- охарактеризовать традиционные и современные методы исследования рисков, методы количественной оценки рисков;
- ознакомить с основными аксиомами и элементами современной теорией рисков и существующими концепциями риска;
- представить порядок проведения исследования рисков;
- охарактеризовать ценность информации в рискованных ситуациях;
- охарактеризовать критерии выбора в рискованных ситуациях;
- изучить методы моделирования рискованных ситуаций и обоснования решений;
- получение практических навыков идентификации рисков, сопровождающих те или иные виды деятельности в сфере информационной безопасности, связанных с той или иной ситуацией, формализации рискованных ситуаций, выбора методов оценки рисков и принятия решений.

Таблица 6.2 Показатели и критерии определения уровня сформированности компетенций (частей компетенций)

№ п/п	Код компетенции (или её части)	Уровни сформированности компетенции		
		Пороговый (удовлетворительный)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
1	ОПК-1	Знать: - методологию	Знать: - основы культуры	Знать: - основные положения и методы

		<p>исследовательской деятельности, основные проблемы в области информационной безопасности;</p> <p>Уметь:</p> <ul style="list-style-type: none"> - определять программу проведения исследований, <p>Владеть:</p> <ul style="list-style-type: none"> - планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач 	<p>научного исследования в информационной безопасности,</p> <p>Уметь:</p> <ul style="list-style-type: none"> - использовать и применять их в современных информационно-коммуникационных технологиях <p>Владеть:</p> <ul style="list-style-type: none"> - способностью к критическому анализу результатов научного творчества 	<p>социальных, гуманитарных и экономических наук при решении педагогических задач</p> <p>Уметь:</p> <ul style="list-style-type: none"> - использовать теоретический материал в педагогической, научно-исследовательской, творческой, управленческой деятельности <p>Владеть:</p> <ul style="list-style-type: none"> - организационными формами и методами проведения научных исследований;
2	ОПК-3	<p>Знать:</p> <ul style="list-style-type: none"> - стандарты в области информационной безопасности; <p>Уметь:</p> <ul style="list-style-type: none"> - сопоставлять характеристики объекта информатизации действующим стандартам, <p>Владеть:</p> <ul style="list-style-type: none"> - комплексной оценки защищённости объекта информатизации 	<p>Знать:</p> <ul style="list-style-type: none"> - методологические подходы применения нормативных документов при оценке защищённости объектов информатизации, <p>Уметь:</p> <ul style="list-style-type: none"> - выявлять недекларируемые угрозы объекту информатизации <p>Владеть:</p> <ul style="list-style-type: none"> - способностью к критическому анализу используемых методов аудита информационной безопасности 	<p>Знать:</p> <ul style="list-style-type: none"> - принципы формирования комплексных отчётов по аудиту информационной безопасности <p>Уметь:</p> <ul style="list-style-type: none"> - вырабатывать методические рекомендации по реализации систем защиты <p>Владеть:</p> <ul style="list-style-type: none"> - организационными формами и методами проведения научных исследований;
3	ПК-1	<p>Знать:</p> <ul style="list-style-type: none"> - аспекты усиления неопределенности и полезности риска; <p>Уметь:</p> <ul style="list-style-type: none"> - выделять критерии классификации рисков и 	<p>Знать:</p> <ul style="list-style-type: none"> - методологические подходы к анализу рисков информационной безопасности, <p>Уметь:</p> <ul style="list-style-type: none"> - представить 	<p>Знать:</p> <ul style="list-style-type: none"> - традиционные и современные методы исследования рисков, методы количественной оценки рисков

		<p>охарактеризовать виды рисков в соответствии с выделенными критериями</p> <p>Владеть:</p> <ul style="list-style-type: none"> - комплексной оценкой рисков нарушения информационной безопасности 	<p>порядок проведения исследования рисков</p> <p>Владеть:</p> <ul style="list-style-type: none"> - методы моделирования рисков ситуаций и обоснования решений 	<p>Уметь:</p> <ul style="list-style-type: none"> - охарактеризовать ценность информации в рискованных ситуациях и критерии выбора в рискованных ситуациях <p>Владеть:</p> <ul style="list-style-type: none"> - методы моделирования рисков ситуаций и обоснования решений; - навыками идентификации рисков, сопровождающих те или иные виды деятельности в сфере информационной безопасности, связанных с той или иной ситуацией, формализации рисков ситуаций, выбора методов оценки рисков и принятия решений
4	ПК-2	<p>Знать:</p> <ul style="list-style-type: none"> - аспекты усиления неопределенности и полезности риска; <p>Уметь:</p> <ul style="list-style-type: none"> - выделять критерии классификации рисков и охарактеризовать виды рисков в соответствии с выделенными критериями <p>Владеть:</p> <ul style="list-style-type: none"> - комплексной оценкой рисков нарушения информационной безопасности 	<p>Знать:</p> <ul style="list-style-type: none"> - методологические подходы к анализу рисков информационной безопасности, <p>Уметь:</p> <ul style="list-style-type: none"> - представить порядок проведения исследования рисков <p>Владеть:</p> <ul style="list-style-type: none"> - методы моделирования рисков ситуаций и обоснования решений 	<p>Знать:</p> <ul style="list-style-type: none"> - традиционные и современные методы исследования рисков, методы количественной оценки рисков <p>Уметь:</p> <ul style="list-style-type: none"> - охарактеризовать ценность информации в рискованных ситуациях и критерии выбора в рискованных ситуациях <p>Владеть:</p> <ul style="list-style-type: none"> - методы

				<p>моделирования рисков ситуаций и обоснования решений;</p> <ul style="list-style-type: none"> – навыками идентификации рисков, сопровождающих те или иные виды деятельности в сфере информационной безопасности, связанных с той или иной ситуацией, формализации рисков ситуаций, выбора методов оценки рисков и принятия решений
5	УК-1	<p>Знать:</p> <ul style="list-style-type: none"> -методологию исследовательской деятельности, основные проблемы в области информационной безопасности; <p>Уметь:</p> <ul style="list-style-type: none"> - определять программу проведения исследований, <p>Владеть:</p> <ul style="list-style-type: none"> - планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач 	<p>Знать:</p> <ul style="list-style-type: none"> - основы культуры научного исследования в информационной безопасности, <p>Уметь:</p> <ul style="list-style-type: none"> - использовать и применять их в современных информационно-коммуникационных технологиях <p>Владеть:</p> <ul style="list-style-type: none"> - способностью к критическому анализу результатов научного творчества 	<p>Знать:</p> <ul style="list-style-type: none"> - основные положения и методы социальных, гуманитарных и экономических наук при решении педагогических задач <p>Уметь:</p> <ul style="list-style-type: none"> - использовать теоретический материал в педагогической, научно-исследовательской, творческой, управленческой деятельности <p>Владеть:</p> <ul style="list-style-type: none"> -организационными формами и методами проведения научных исследований;

6.3 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

Таблица 6.3 Паспорт комплекта оценочных средств

№ п/п	Раздел (тема) дисциплины	Код компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкалоценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1	Введение. Базовые вопросы управления ИБ.	ОПК1	Лекция Практическое занятие	См. МУ	1	<p>Оценивая ответ, члены комиссии учитывают следующие <i>основные критерии</i>:</p> <ul style="list-style-type: none"> – уровень теоретических знаний (подразумевается не только формальное воспроизведение информации, но и понимание предмета, которое подтверждается правильными ответами на дополнительные, уточняющие вопросы, заданные членами комиссии); – умение использовать теоретические знания при анализе конкретных проблем, ситуаций; – качество изложения материала, то есть обоснованность, четкость, логичность ответа, а также его полнота (то есть содержательность, не исключающая сжатости); - способность устанавливать внутри- и межпредметные связи, оригинальность и красота мышления, знакомство с дополнительной литературой и множество других факторов. <p><i>Критерии оценок:</i> Оценка <i>зачтено</i> – исчерпывающее владение программным материалом, понимание сущности рассматриваемых процессов и</p>
		ОПК-3	Лекция Практическое занятие	См. МУ	2	
2	Оценочные стандарты в информационно й безопасности	ОПК-1 ОПК-3 ПК-1 ПК-2	Лекция	См. МУ	3	
		ОПК-1 ОПК-3 ПК-1 ПК-2	Практическое занятие	См. МУ	4	
3	Стандарты управления информационно й безопасностью	ОПК-1 ОПК-3 ПК-1 ПК-2	Лекция Практическое занятие	См. МУ	5	
		ОПК-1 ОПК-3 ПК-1 ПК-2 УК-1	Лекция Практическое занятие			
4	Создание СУИБ на предприятии	ОПК-1 ОПК-3 ПК-1 ПК-2	Лекция Практическое занятие	См. МУ	6	
		ОПК-1 ОПК-3 ПК-1 ПК-2 УК-1	Лекция Практическое занятие			

5	Анализ рисков информационно й безопасности компании		Лекция Практическ оезаяние	См. МУ	7	явлений, твёрдое знание основных положений дисциплины, умение применять концептуальный аппарат при анализе актуальных проблем. Логически последовательные, содержательные, конкретные ответы на все вопросы экзаменационного билета и на дополнительные вопросы членов комиссии, свободное владение источниками. Предложенные в качестве самостоятельной работы формы работы (примерный план исследовательской деятельности; пробная рабочая программа) приняты без замечаний.
			Лекция Практическ оезаяние			
6	Методика оценки рисков информационно й безопасности компании	ОПК-1 ОПК-3 ПК-1 ПК-2 УК-1	Лекция Практическ оезаяние	См. МУ	8	Оценка не зачтено – отсутствие ответа хотя бы на один из основных вопросов, либо грубые ошибки в ответах, полное непонимание смысла проблем, не достаточно полное владение терминологией. Отсутствие выполненных самостоятельных дополнительных работ.
		ОПК-1 ОПК-3 ПК-1 ПК-2 УК-1	Лекция Практическ оезаяние			
7	Методики и технологии управления рисками	ОПК-1 ОПК-3 ПК-1 ПК-2 УК-1	Лекция Практическ оезаяние	См. МУ	9	Оценка по дисциплине «Методы анализа рисков нарушения информационной безопасности» складывается из зачета самостоятельных работ и оценки ответа на зачете.
		ОПК-1 ОПК-3 ПК-1 ПК-2 УК-1	Лекция Практическ оезаяние			
8	Разработка корпоративной методики анализа рисков	ОПК-1 ОПК-3 ПК-1 ПК-2	Лекция Практическ оезаяние	См. МУ	10	Показатели и критерии оценивания компетенций (результатов): Процедура испытания предусматривает ответ аспиранта по вопросам зачетного билета, который заслушивает комиссия. После сообщения аспиранта и ответов на заданные вопросы, комиссия обсуждает качество ответа и голосованием принимает решение об оценке (зачтено/не зачтено), вносимой в протокол. Особое внимание обращается на степень осмысления процессов развития методологии науки и ее
		ОПК-1 ОПК-3 ПК-1 ПК-2	Лекция Практическ оезаяние	См. МУ		
9	Современные методы и средства анализа и управление рисками информационных систем компаний	ОПК-1 ОПК-3 ПК-1 ПК-2	Лекция Практическ оезаяние	См. МУ	11	
		ОПК-1 ОПК-3 ПК-1 ПК-2 УК-1	Лекция Практическ оезаяние			

						<p>современных проблем. Изучаемый материал должен быть понятным. Приоритет понимания обуславливает способность изложения собственной точки зрения в контексте с другими позициями.</p>
--	--	--	--	--	--	---

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- Список методических указаний, используемых в образовательном процессе, представлен в п. 7.2;
- Оценочные средства представлены в учебно-методическом комплексе дисциплины.

1. Собеседование

Вопросы:

1. Сущность и функции управления
2. Наука управления.
3. Принципы, подходы и виды управления.
4. Цели и задачи управления ИБ.
5. Понятие системы управления.

2. Лекция с элементами проблемного изложения по вопросу: Использование результатов анализа рисков ИБ.

3. Сообщение студента.

Тема: Внедрение разработанных процессов. Документ «Положение о применимости»

4. Коллоквиум

Вопросы:

1. Качественные методики управления рисками.
2. Анализ причинно-следственной природы информационных рисков.
3. Политика управления информационными рисками
4. Система управления информационными рисками
5. Повышение эффективности системы управления рисками
6. Создание централизованного иерархического управления

5. Сообщение студента.

Тема: Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

6. Круглый стол «Оценка уровня защищенности информационных процессов»

7. Опрос

1. Введение. Базовые вопросы управления ИБ.
2. Оценочные стандарты в информационной безопасности
3. Создание СУИБ на предприятии
4. Анализ рисков информационной безопасности компании
5. Методика оценки рисков информационной безопасности компании
6. Разработка корпоративной методики анализа рисков
7. Современные методы и средства анализа и управление рисками информационных систем компаний

Рейтинговый контроль не предусмотрен.

Описание оценочных средств и шкал оценивания ответов см. в Таблице 6.3.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная и дополнительная литература

а) основная литература:

1. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.
2. Ищейнов, В.Я. Защита конфиденциальной информации [Текст] : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - Москва : Форум, 2013. - 256 с.
3. Ярочкин, В. И. Аудит безопасности фирмы: теория и практика [Электронный ресурс] : учебное пособие / В. И. Ярочкин, Я. Бузанова. - Москва : Академический Проект|Парадигма, 2012. - 352 с.
4. Богомолов, В.А. Экономическая безопасность [Текст] : учебное пособие / [В. А. Богомолов [и др.] ; под ред. В. А. Богомолова. - 2-е изд., перераб. и доп. - Москва : ЮНИТИ, 2014. - 295 с.
5. Аверченков, В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. - 2-е изд., стер. - М.: Флинта, 2011. - 269 с. // Режим доступа - URL: <http://biblioclub.ru/>

б) дополнительная литература:

1. Ярочкин, В.И. Информационная безопасность [Электронный ресурс]: учебник / В. И. Ярочкин. - 5-е изд. - Москва: Академический проект, 2008. - 544 с.
2. Галатенко, В. А. Основы информационной безопасности. Курс лекций [Текст]: учебное пособие для студентов вузов / Под ред. В. Б. Бетелина. - 2-е изд., испр. - М.: ИНТУИТ. РУ Интернет-университет Информационных Технологий, 2004. - 264 с.
3. Романов, О. А. Организационное обеспечение информационной безопасности [Текст]: учебник / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М.: Академия, 2008. - 192 с.
4. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие. / Ю.Н. Загинайлов. - М.; Берлин: Директ-Медиа, 2015. // Режим доступа - URL: <http://biblioclub.ru/>
5. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / С.А. Нестеров; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб: Издательство Политехнического университета, 2014. - 322 с. // Режим доступа - URL: <http://biblioclub.ru/>
6. Правовое обеспечение информационной безопасности [Текст]: учебное пособие / под ред. С. Я. Казанцева. - 3-е изд., стер. - М.: Академия, 2008. - 240 с.
7. Галатенко, В. А. Стандарты информационной безопасности [Текст]: курс лекций / под ред. В. Б. Бетелина. - М.: ИНТУИТ. РУ Интернет-университет Информационных Технологий, 2004. - 328 с.
8. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. - Орел: МАБИВ, 2014. - 257 с. // Режим доступа - URL: <http://biblioclub.ru/>

7.2 Перечень методических указаний

1. Организация работы групповых политик безопасности WINDOWS 8.1 PROFESSIONAL [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Методы и средства защиты информации в системах электронного документооборота» для студентов специальностей и направлений подготовки 090104.65, 090900.62, 090303.65, 090900.68. / Юго-Зап. гос. ун-т ; сост.: И. В. Калуцкий, И. С. Надеина. - Электрон.текстовые дан. (4427 КБ). - Курск : ЮЗГУ, 2014. - 46 с.

7.3 Перечень ресурсов информационно-телекоммуникационной сети Интернет

12. <http://school-collection.edu.ru/> - федеральное хранилище Единая коллекция цифровых образовательных ресурсов

13. <http://www.edu.ru/> - федеральный портал Российское образование

14. www.edu.ru – сайт Министерства образования РФ

15. <http://www.iqlib.ru> – электронная библиотека образовательных и просветительных изданий

16. <http://www.lib.msu.su/index.html> - Научная библиотека Московского государственного университета им. М.В.Ломоносова

17. <http://elibrary.ru/defaultx.asp> - научная электронная библиотека «Elibrary»

7.4 Перечень информационных технологий

Microsoft Office Power Point;

Microsoft Office Excel;

Диспетчер рисунков Microsoft Office: (Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал».)

8 Материально-техническое обеспечение дисциплины

Для обеспечения учебного процесса используются: лекционная аудитория, оснащенная мультимедийными средствами, аудитория для практических занятий, компьютерная аудитория, обеспечивающая выход в ИНТЕРНЕТ.

8 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

№ изменения	Номера страниц				Всего	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			
1	2	3	4	5	6	7	8
1		4			1	01.09.17	Приказ ФГБОУ «Юго-Западный государственный университет» № 576 от 31.08.2017 г. « О внесении изменений в приказ №263 от 29.03.2017 г. « Об утверждении норм времени для расчета учебной и других видов работы»
2		9			1	01.09.17	Приказ № 301 от 05.04.2017 г.
3		19-20			2	13.12.17	Протокол заседания кафедры ИСиТ №10 от 13.12.17

Приложение А

Вопросы к зачету по дисциплине «Методы анализа рисков нарушения информационной безопасности»

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность.
17. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения.

Приложение Б

Методические указания для выполнения самостоятельной работы

Самостоятельная работа аспирантов направлена на:

- 1) выработку навыков восприятия и анализа философских и методологических проблем естественных, информационных и технических дисциплин на основе научных текстов;
- 2) совершенствование навыков методологического подхода к восприятию научных текстов и критического отношения к источникам информации;
- 3) знание специфики эмпирического и теоретического уровней научного исследования и содержание основных методов, используемых на этих уровнях;
- 4) развитие и совершенствование способностей к конструктивному диалогу, к дискуссии, к формированию логической аргументации и обоснованию собственной позиции по тому или иному вопросу.

Закрепление основных позиций в рамках дисциплины «Методология науки и образовательной деятельности» должно строиться на понимании связи науки с философией, искусством, религией, социальной и практической деятельностью, а также с проблемами собственной специальности. Предполагается применение активных методов обучения, т.е. способы активизации учебно-познавательной деятельности аспирантов, которые побуждают их к активной мыслительной и практической деятельности в процессе овладения материалом. Активные методы обучения предполагают использование тематических таблиц и схем по учебной литературе, Интернет-материалов и лекций преподавателя, позволяющие оценить умение аспиранта работать с учебной литературой (выбирать, структурировать информацию, размещать её в хронологической последовательности).

Проверка выполнения заданий осуществляется как на семинарских занятиях с помощью устных выступлений и их коллективного обсуждения, так и с помощью письменных самостоятельных (контрольных) работ.

Для развития и совершенствования коммуникативных способностей аспирантов, навыков участия в конструктивном диалоге организуются специальные учебные занятия в виде «деловых игр», «диспутов» или «конференций», при подготовке к которым студенты заранее распределяются по группам, отстаивающим ту или иную точку зрения по обсуждаемой проблеме. Одним из видов самостоятельной работы является написание творческой работы по заданной либо согласованной с преподавателем теме. *Творческая работа (доклад с презентацией)* представляет собой оригинальное произведение объемом до 10 страниц печатного текста (10-15 слайдов), в данном случае предложено составление примерной

индивидуальной программы научного исследования. Творческая работа не является рефератом, и не должна носить описательный характер. В ней желательно сосредоточить внимание на критическом анализе рассматриваемого материала и изложении своей точки зрения на проблему, что будет способствовать развитию творческих способностей. Так же в качестве самостоятельного задания аспирант подготавливает примерный образец рабочей программы по профилирующему предмету, т.к. первое, с чем ему придется столкнуться при вхождении в профессию (даже на уровне педагогической практики) – это разработка блоков учебно-методического комплекса. При подготовке примерной рабочей программы аспирант учиться работать с нормативными документами – стандартами, учебными рабочими планами, локальными приказами и положениями и т.д., что должно максимально полно помочь ему ориентироваться в этих вопросах в будущей преподавательской деятельности.