Минобрнауки России
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Проректор по учебной работе

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

_____ Василенко В.Н.

«25» мая 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ

Направление подготовки

09.04.02 Информационные системы и технологии

Направленность (профиль) подготовки

Информационные технологии в корпоративном управлении

Квалификация выпускника

Магистр

1. Цели и задачи дисциплины

Целями освоения дисциплины «Управление информационными рисками» является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности:

01 Образование и наука (в сфере научных исследований в области информатики и вычислительной техники)

06 Связь, информационные и коммуникационные технологии (в сфере исследования, разработки, внедрения и сопровождения информационных процессов, технологий, систем и сетей, их инструментальное (программное, техническое, организационное) обеспечение)

40 Сквозные виды профессиональной деятельности

Дисциплина направлена на решение задач профессиональной деятельности следующих типов:

- научно-исследовательский;

- производственно-технологический;

- организационно-управленческий;

- проектный.

Программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.04.02 Информационные системы и технологии, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 917 (с изменениями №1456 от 26.11.2020).

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

№ п/п	Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции
1	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИД1$_{УК-1}$ - Анализирует поставленную задачу и осуществляет поиск необходимой информации для ее решения
			ИД2$_{УК-1}$ – Решает поставленные задачи, используя системный подход, на основе критического анализа и синтеза информации и оценивает последствия возможных решений
2	ПКв-4	Способность управлять проектами в области ИТ малого и среднего уровня сложности в условиях неопределенностей, порождаемых запросами на изменения, с применением формальных инструментов управления рисками и проблемами проекта	ИД1$_{ПКв-4}$ – Планирование конфигурационного управления в проектах малого и среднего уровня сложности в области ИТ
			ИД2 $_{ПКв-4}$ – Командообразование и развитие команды проекта малого и среднего уровня сложности в области ИТ
			ИД2$_{ПКв-4}$ – Планирование управления рисками в проектах малого и среднего уровня сложности в области ИТ

Код и наименование индикатора достижения компетенции	**Результаты обучения (показатели оценивания)**
ИД1$_{УК-1}$ - Анализирует поставленную задачу и осуществляет поиск необходимой информации для ее решения	Знает: стандарты безопасности информационных технологий Аспекты безопасности информации
	Умеет: отражать атаки и защищать информацию от случайных угроз
	Владеет: моделями оценки величины рисков
ИД2$_{УК-1}$ – Решает поставленные задачи, используя системный подход, на основе критического анализа и синтеза информации и оценивает последствия возможных	Знает: основные этапы проектирования проекта, систему оценки и инструменты управления проектом
	Умеет: Инструментами поддержки оперативного управления проектом.
	Владеет: Сетевым анализом проекта исходя из действующих

решений	правовых норм, имеющихся ресурсов и ограничений
ИД2 $_{ПКв-4}$ – Командообразование и развитие команды проекта малого и среднего уровня сложности в области ИТ	Знает: Функции службы информационной безопасности
	Умеет: организовать защиту информации
	Владеет: навыками обработки основных категорий персональных данных
ИД1$_{ПКв-4}$ – Планирование конфигурационного управления в проектах малого и среднего уровня сложности в области ИТ	Знает: простейшие модели прогнозирования экономических характеристик программного продукта
	Умеет: применять на практике экспертное прогнозирование экономических характеристик программного продукта
	Владеет: навыками оценки управления проекта
ИД3$_{ПКв-4}$ – Планирование управления рисками в проектах малого и среднего уровня сложности в области ИТ	Знает: показатели оценки проектных решений, алгоритм оценки проекта
	Умеет: приметить методики моделирования трендов состояния сложных объектов
	Владеет: навыками оценки сложности проекта на основе структурных моделей

3. Место дисциплины (модуля) в структуре ОП ВО

Дисциплина относится к обязательной части Блока 1 «Дисциплины/модули» ОП ВО, модуль «Обязательный». Дисциплина является обязательной к изучению.

Изучение дисциплины основано на знаниях, умениях и навыках, сформированных при изучении программы бакалавриата по направлению 09.03.02 «Информационные системы и технологии».

Дисциплина является предшествующей для *следующих видов дисциплин и практик* Современные проблемы информационных технологий Управление информационными рисками Учебная практика, ознакомительная практика, Производственная практика, преддипломная практика

4. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины (модуля) составляет 5 зачетных единицы

Виды учебной работы	**Всего ак. ч.**	**Распределение трудоемкости по семестрам, ак.ч.**
		1 семестр
Общая трудоемкость дисциплины (модуля)	**180**	**180**
Контактная работа в т. ч. аудиторные занятия:	**54,05**	**54,05**
Лекции	17	17
в том числе в форме практической подготовки	-	-
Лабораторные работы	34	34
в том числе в форме практической подготовки	*34*	*34*
Консультации текущие	*0,85*	*0,85*
Консультация	0,2	0,2
Консультация перед экзаменом	2	2
Вид аттестации (экзамен)	**33,8**	**33,8**
Самостоятельная работа:	**92,15**	**92,15**
Проработка материалов по лекциям	7,15	7,15
Проработка материалов по учебникам, учебным пособиям	16	16
Домашнее задание	27	27
Выполнение расчетов для лабораторных работ	25	25
Подготовка к выполнению тестовых заданий	17	17

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины (модуля)

№ п/п	Наименование раздела дисциплины	Содержание раздела	Трудоемкость раздела, ч
1	Информационная безопасность и безопасность информации	Стандарты безопасности информационных технологий. Термины и определения для безопасности информации. Аспекты безопасности информации. Конфиденциальность информации и ее доступность. Целостность информации и ее контроль. Основные понятия и определения. Основные виды угроз. Характеристика и классификация атак.	34,15
2	Цели и функции системы защиты информации	Защита информации от случайных угроз. Защита информации от побочных излучений. Риск как разновидность неопределенности. Модели оценки величины рисков. Трехфакторная модель оценки информационных рисков. Методы оценки субъективных вероятностей. Стандарты управления информационной безопасности.	35
3	Управление рисками информационной безопасности	Программные средства, поддерживающие аудит информационной безопасности. Правовое обеспечение защиты информации. Организационное обеспечение защиты информации. Функции органов государственной власти, обеспечивающих информационную безопасность в Российской Федерации. Функции службы информационной безопасности. Основные понятия и определения. Обработка персональных данных. Обработка основных категорий персональных данных. Уровни защищенности и виды ИСПДн. Состав мер защиты персональных данных. Классификация государственных информационных систем. Определение актуальных угроз безопасности информации. Разработка модели нарушителя. Определение актуальных угроз для информационной системы.	38
4	Криптографические методы защиты целостности и конфиденциальности электронных документов	Основные понятия криптографии. Поточное шифрование. Общие сведения о симметричных блочных криптосистемах. Схема Фейстеля. Алгоритм DES и его развитие. Стандарт криптографической защиты AES. Национальные стандарты РФ. Алгоритм криптографического преобразования (ГОСТ 28147-89)	36
		Консультации перед экзаменом	*2,0*
		Консультации текущие	*0,85*
		Экзамен	*0,2*
		Вид аттестации – экзамен	*33,8*

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ, час	СРО, час
1	Информационная безопасность и безопасность информации	4	8	22,15
2	Цели и функции системы защиты информации	4	8	23
3	Управление рисками информационной безопасности	5	10	23
4	Криптографическиеметоды защиты целостности и конфиденциальности электронных документов	4	8	24
	Консультации перед экзаменом		*2,0*	
	Консультации текущие		*0,85*	
	Экзамен		*0,2*	
	Вид аттестации – экзамен		*33,8*	

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Содержание раздела	Трудоемкость раздела, ч
1	Информационная безопасность и безопасность информации	Стандарты безопасности информационных технологий. Термины и определения для безопасности информации. Аспекты безопасности информации. Конфиденциальность информации и ее доступность. Целостность информации и ее контроль. Основные понятия и определения. Основные виды угроз. Характеристика и классификация атак.	4
2	Цели и функции системы защиты информации	Защита информации от случайных угроз. Защита информации от побочных излучений. Риск как разновидность неопределенности. Модели оценки величины рисков. Трехфакторная модель оценки информационных рисков. Методы оценки субъективных вероятностей. Стандарты управления информационной безопасности.	4
3	Управление рисками информационной безопасности	Программные средства, поддерживающие аудит информационной безопасности. Правовое обеспечение защиты информации. Организационное обеспечение защиты информации. Функции органов государственной власти, обеспечивающих информационную безопасность в Российской Федерации. Функции службы информационной безопасности. Основные понятия и определения. Обработка персональных данных. Обработка основных категорий персональных данных. Уровни защищенности и виды ИСПДн. Состав мер защиты персональных данных. Классификация государственных информационных систем. Определение актуальных угроз безопасности информации. Разработка модели нарушителя. Определение актуальных угроз для информационной системы.	5
4	Криптографическиеметоды защиты целостности и конфиденциальности электронных документов	Основные понятия криптографии. Поточное шифрование. Общие сведения о симметричных блочных криптосистемах. Схема Фейстеля. Алгоритм DES и его развитие. Стандарт криптографической защиты AES. Национальные стандарты РФ. Алгоритм криптографического преобразования (ГОСТ 28147-89)	4

5.2.2 Практические занятия (семинары)

№ п/п	Наименование раздела дисциплины	Содержание раздела	Трудоемкость раздела, ч
1	Информационная безопасность и безопасность информации	Стандарты безопасности информационных технологий. Термины и определения для безопасности информации. Аспекты безопасности информации. Конфиденциальность информации и ее доступность. Целостность информации и ее контроль. Основные понятия и определения. Основные виды угроз. Характеристика и классификация атак.	8
2	Цели и функции системы защиты информации	Защита информации от случайных угроз. Защита информации от побочных излучений. Риск как разновидность неопределенности. Модели оценки величины рисков. Трехфакторная модель оценки информационных рисков. Методы оценки субъективных вероятностей. Стандарты управления информационной безопасности.	8
3	Управление рисками информационной	Программные средства, поддерживающие аудит информационной безопасности. Правовое	10

	безопасности	обеспечение защиты информации. Организационное обеспечение защиты информации. Функции органов государственной власти, обеспечивающих информационную безопасность в Российской Федерации. Функции службы информационной безопасности. Основные понятия и определения. Обработка персональных данных. Обработка основных категорий персональных данных. Уровни защищенности и виды ИСПДн. Состав мер защиты персональных данных. Классификация государственных информационных систем. Определение актуальных угроз безопасности информации. Разработка модели нарушителя. Определение актуальных угроз для информационной системы.	
4	Криптографические методы защиты целостности и конфиденциальности электронных документов	Основные понятия криптографии. Поточное шифрование. Общие сведения о симметричных блочных криптосистемах. Схема Фейстеля. Алгоритм DES и его развитие. Стандарт криптографической защиты AES. Национальные стандарты РФ. Алгоритм криптографического преобразования (ГОСТ 28147-89)	8

5.2.3 Лабораторный практикум - *Не предусмотрен*

5.2.4 Самостоятельная работа обучающихся

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, ч
1	Информационная безопасность и безопасность информации	Проработка материалов по лекциям	1,15
		Проработка материалов по учебникам, учебным пособиям	4
		Домашнее задание	6
		Выполнение расчетов для лабораторных работ	7
		Подготовка к выполнению тестовых заданий	4
2	Цели и функции системы защиты информации	Проработка материалов по лекциям	2
		Проработка материалов по учебникам, учебным пособиям	4
		Домашнее задание	7
		Выполнение расчетов для лабораторных работ	6
		Подготовка к выполнению тестовых заданий	
3	Управление рисками информационной безопасности	Проработка материалов по лекциям	2
		Проработка материалов по учебникам, учебным пособиям	4
		Домашнее задание	7
		Выполнение расчетов для лабораторных работ	6
		Подготовка к выполнению тестовых заданий	4
3	Криптографические методы защиты целостности и конфиденциальности электронных документов	Проработка материалов по лекциям	2
		Проработка материалов по учебникам, учебным пособиям	4
		Домашнее задание	7
		Выполнение расчетов для лабораторных работ	6
		Подготовка к выполнению тестовых заданий	5

6 Учебно-методическое и информационное обеспечение дисциплины (модуля)

Для освоения дисциплины обучающийся может использовать:

6.1 Основная литература

Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов. — Санкт-Петербург : Лань, 2021 https://e.lanbook.com/book/156401

Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие. — Самара : ПГУТИ, 2018 https://e.lanbook.com/book/182299

Риск-модели информационной безопасности : учебное пособие / А. А. Корниенко, С. В. Корниенко, А. П. Глухов, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2021 https://e.lanbook.com/book/191006

6.2 Дополнительная литература

Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279

Панова, Т. В. Управление техносферной безопасностью : методические указания / Т. В. Панова, М. В. Панов. — Брянск : Брянский ГАУ, 2019. — 132 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/133122

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] : методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж : ВГУИТ, 2015. – Режим доступа : http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813. - Загл. с экрана

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	*https://www.edu.ru/*
Научная электронная библиотека	*https://elibrary.ru/defaultx.asp?*
Национальная исследовательская компьютерная сеть России	*https://niks.su/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*https://minobrnauki.gov.ru/*
Портал открытого on-line образования	*https://npoed.ru/*
Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ	*https://education.vsuet.ru/*

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины используется программное обеспечение, современные профессиональные базы данных и информационные справочные системы: ЭИОС университета, в том числе на базе программной платформы «Среда электронного обучения 3KL», автоматизированная информационная база «Интернет-тренажеры», «Интернет-экзамен».

При освоении дисциплины используется лицензионное и открытое программное обеспечение:

Программы	Лицензии, реквизиты подтверждающего документа
Microsoft Windows 7 (64 - bit)	Microsoft Windows Professional 7 Russian Upgrade Academic OPEN 1 License No Level #47881748 от 24.12.2010 г. http://eopen.microsoft.com
Microsoft Windows 8.1 (64 - bit)	Microsoft Open License Microsoft Windows Professional 8 Russian Upgrade Academic OPEN 1 License No Level#61280574 от 06.12.2012 г. http://eopen.microsoft.com
Microsoft Office Professional Plus 2010	Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 License No Level #48516271 от 17.05.2011 г. http://eopen.microsoft.com
Microsoft Office 2007	Microsoft Office 2007 Russian Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com
Microsoft Office 2010	Microsoft Office 2010 Russian Academic OPEN 1 License No Level #47881748 от 24.12.2010 г. http://eopen.microsoft.com
AdobeReaderXI	(бесплатное ПО) https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader/volumedistribution.htm
Альт Образование 8.2 + LibreOffice 6.2+Maxima	Лицензия № AAA.0217.00 с 21.12.2017 г. по «Бессрочно»

7 Материально-техническое обеспечение дисциплины (модуля)

Необходимый для реализации образовательной программы перечень материально-технического обеспечения включает:

лекционные аудитории (оборудованные видеопроекционным оборудованием для презентаций; средствами звуковоспроизведения; экраном; имеющие выход в Интернет);

помещения для проведения семинарских, лабораторных и практических занятий (оборудованные учебной мебелью);

библиотеку (имеющую рабочие места для студентов, оснащенные компьютерами с доступом к базам данных и Интернет);

компьютерные классы.

Обеспеченность процесса обучения техническими средствами полностью соответствует требованиям ФГОС по направлению 09.03.02. Материально-техническая база приведена в лицензионных формах и расположена во внутренней сети по адресу http://education.vsuet.ru.

Аудитории для проведения учебных занятий:

Учебная аудитория для проведения учебных занятий № 401	Комплект мебели для учебного процесса. Мультимедийный проектор Epson EH-TW650; настенный экран.

Аудитории для проведения учебных занятий:

Учебная аудитория для проведения учебных занятий № 151	Комплект мебели для учебного процесса, Рабочие станции 12 шт (IntelCorei3-540)
Учебная аудитория для проведения учебных занятий № 134	Комплект мебели для учебного процесса, Рабочие станции 12 шт (IntelCorei3-540)

Аудитория для самостоятельной работы обучающихся

Учебная аудитория для самостоятельной работы обучающихся № 337	Комплект мебели для учебного процесса, Рабочие станции 12 шт (Intel Core 2 DuoE7300)

Дополнительно самостоятельная работа обучающихся может осуществляться при использовании:

Читальные залы библиотеки.	Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами.

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине (модулю)

Оценочные материалы (ОМ) для дисциплины (модуля) включают в себя:

- перечень компетенций с указанием индикаторов достижения компетенций, этапов их формирования в процессе освоения образовательной программы;
- описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.

ОМ представляются отдельным комплектом и входят в состав рабочей программы дисциплины (модуля).

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

ПРИЛОЖЕНИЕ
к рабочей программе

1. Организационно-методические данные дисциплины для заочной форм обучения

1.1 Объемы различных форм учебной работы и виды контроля в соответствии с учебным планом (заочная форма)

Общая трудоемкость дисциплины (модуля) составляет 5 зачетных единиц

Виды учебной работы	**Всего ак. ч.**	**Распределение трудоемкости по семестрам, ак. ч.**
		2 курс 4 семестр
Общая трудоемкость дисциплины (модуля)	**180**	**180**
Контактная работа в т. ч. аудиторные занятия:	**21,9**	**21,9**
Лекции	6	6
Практические занятия	12	12
в том числе в форме практической подготовки	-	-
Консультации текущие	0,9	0,9
Рецензирование контрольной работы	0,8	0,8
Консультация перед экзаменом	2,0	2,0
Вид аттестации (экзамен)	0,2	0,2
Самостоятельная работа:	**151,3**	**151,3**
Проработка материалов по лекциям	3,3	3,3
Проработка материалов по учебникам, учебным пособиям	90	90
Контрольная работа	10	10
Домашняя работа	11	11
Выполнение расчетов для практических работ	12	12
Подготовка к выполнению тестовых заданий	25	25
Подготовка к экзамену	**6,8**	**6,8**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции
1	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИД1$_{УК-1}$ - Анализирует поставленную задачу и осуществляет поиск необходимой информации для ее решения
			ИД2$_{УК-1}$ – Решает поставленные задачи, используя системный подход, на основе критического анализа и синтеза информации и оценивает последствия возможных решений
2	ПКв-4	Способность управлять проектами в области ИТ малого и среднего уровня сложности в условиях неопределенностей, порождаемых запросами на изменения, с применением формальных инструментов управления рисками и проблемами проекта	ИД1$_{ПКв-4}$ – Планирование конфигурационного управления в проектах малого и среднего уровня сложности в области ИТ
			ИД2 $_{ПКв-4}$ – Командообразование и развитие команды проекта малого и среднего уровня сложности в области ИТ
			ИД2$_{ПКв-4}$ – Планирование управления рисками в проектах малого и среднего уровня сложности в области ИТ

Код и наименование индикатора достижения компетенции	**Результаты обучения (показатели оценивания)**
ИД1$_{УК-1}$ - Анализирует поставленную задачу и осуществляет поиск необходимой информации для ее решения	Знает: стандарты безопасности информационных технологий Аспекты безопасности информации
	Умеет: отражать атаки и защищать информацию от случайных угроз
	Владеет: моделями оценки величины рисков
ИД2$_{УК-1}$ – Решает поставленные задачи, используя системный подход, на основе критического анализа и синтеза информации и оценивает последствия возможных решений	Знает: основные этапы проектирования проекта, систему оценки и инструменты управления проектом
	Умеет: Инструментами поддержки оперативного управления проектом.
	Владеет: Сетевым анализом проекта исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИД2 $_{ПКв-4}$ – Командообразование и развитие команды проекта малого и среднего уровня сложности в области ИТ	Знает: Функции службы информационной безопасности
	Умеет: организовать защиту информации
	Владеет: навыками обработки основных категорий персональных данных
ИД1$_{ПКв-4}$ – Планирование конфигурационного управления в проектах малого и среднего уровня сложности в области ИТ	Знает: простейшие модели прогнозирования экономических характеристик программного продукта
	Умеет: применять на практике экспертное прогнозирование экономических характеристик программного продукта
	Владеет: навыками оценки управления проекта
ИД3$_{ПКв-4}$ – Планирование управления рисками в проектах малого и среднего уровня сложности в области ИТ	Знает: показатели оценки проектных решений, алгоритм оценки проекта
	Умеет: приметить методики моделирования трендов состояния сложных объектов
	Владеет: навыками оценки сложности проекта на основе структурных моделей

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства		Технология/процедура оценивания (способ контроля)
			Наименование	№№ заданий	
1	Общие сведения о сетях и системах передачи	УК-1 ПКв-4	Тест		Компьютерное тестирование
			Собеседование		Проверка

	информации		(вопросы для зачета)		преподавателем
			Подготовка к практическим работам		Компьютерное тестирование
2	Компьютерные технологии и системы связи	УК-1 ПКв-4	Тест		Компьютерное тестирование
			Собеседование (вопросы для зачета)		Проверка преподавателем Отметка в системе «зачтено – не зачтено»
			Подготовка к практическим работам		Компьютерное тестирование
3	Волоконно-оптические линии в компьютерных сетях и системах передачи информации	УК-1 ПКв-4	Тест		Компьютерное тестирование
			Собеседование (вопросы для зачета)		Проверка преподавателем
			Подготовка к практическим работам		Компьютерное тестирование
4	Антенно-фидерные устройства в сетях и системах передачи информации	УК-1 ПКв-4	Тест		Компьютерное тестирование
			Собеседование (вопросы для зачета)		Проверка преподавателем
			Подготовка к практическим работам		Компьютерное тестирование
5	Беспроводные компьютерные сети и системы радиосвязи	УК-1 ПКв-4	Тест		Компьютерное тестирование
			Собеседование (вопросы для зачета)		Проверка преподавателем
			Подготовка к практическим работам		Компьютерное тестирование
6	Информационная безопасность в компьютерных сетях и системах передачи информации	УК-1 ПКв-4	Тест		Компьютерное тестирование
			Собеседование (вопросы для зачета)		Проверка преподавателем
			Подготовка к практическим работам		Компьютерное тестирование

3 Оценочные материалы для промежуточной аттестации

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

Для оценки знаний, умений, навыков студентов по дисциплине применяется балльно-рейтинговая система оценки сформированности компетенций студента.

Бально-рейтинговая система оценки осуществляется в течение всего семестра при проведении аудиторных занятий и контроля самостоятельной работы. Показателями ОМ являются: текущий опрос в виде собеседования на лабораторных работах, тестовые задания и самостоятельно (домашнее задание). Оценки выставляются в соответствии с графиком контроля текущей успеваемости студентов в автоматизированную систему баз данных (АСУБД) «Рейтинг студентов».

Обучающийся, набравший в семестре более 60 % от максимально возможной бально-рейтинговой оценки работы в семестре получает зачет автоматически.

Студент, набравший за текущую работу в семестре менее 60 %, т.к. не выполнил всю работу в семестре по объективным причинам (болезнь, официальное освобождение и т.п.) допускается до экзамена, однако ему дополнительно задаются вопросы на собеседовании по разделам, выносимым на зачет.

Аттестация обучающегося по дисциплине проводится в форме тестирования и предусматривает возможность последующего собеседования (экзамена). Зачет проводится в виде тестового задания.

Каждый вариант теста включает 30 контрольных заданий, из них:

- 10 контрольных заданий на проверку знаний;
- 10 контрольных заданий на проверку умений;
- 10 контрольных заданий на проверку навыков;

В случае неудовлетворительной сдачи экзамена студенту предоставляется право повторной сдачи в срок, установленный для ликвидации академической задолженности по итогам соответствующей сессии. При повторной сдаче экзамена количество набранных студентом баллов на предыдущем зачете не учитывается.

3.1 Тесты (тестовые задания и кейс-задания)

3.1.1 *Шифр и наименование компетенции*

УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

№ задания	Тестовое задание
	Выбрать один ответ
1.	Команда по разработке политики безопасности обычно включает следующее число человек: 1) от 2 до 5 2) от 2 до 10 3) от 2 до 15 4) от 2 до 20
2.	Количество основных правил глобальной политики безопасности равно: 1) трем 2) четырем 3) пяти 4) шести
3.	В основные обязанности пользователя данными входит следующее их число: 1) два 2) три 3) четыре 4) пять
4.	Какой самый важный вопрос должна решить команда по разработке политики безопасности организации: 1) какие компьютерные и сетевые сервисы требуются для бизнеса 2) зависят ли компьютерные и сетевые сервисы от удаленного доступа к внутренней сети 3) имеется ли требование бизнеса на тот или иной сервис 4) имеются ли требования по доступу к Веб-ресурсам
5.	Основные устанавливаемые роли в безопасности сети включают следующее их количество: 1) два 2) три 3) четыре 4) пять
6.	Процедура управления конфигурацией определяет: 1) какую информацию следует регистрировать и прослеживать 2) как тестируется и инсталлируется новое аппаратное обеспечение 3) как тестируется и инсталлируется новое программное обеспечение 4) кто должен быть проинформирован, когда вносятся изменения в различные виды обеспечения
7.	Первые шаги по разработке политики безопасности включают следующее их число: 1) три 2) четыре 3) пять 4) шесть
8.	Процедура реагирования на события определяет: 1) какую информацию следует регистрировать и прослеживать 2) кто имеет полномочия выполнять изменения конфигурации аппаратного и программного обеспечения 3) как обрабатывать исследование отклонений от нормы 4) как следует реагировать на атаки вторжения
9.	На этапе анализа рисков осуществляются следующее число действий:

	1) три 2) четыре 3) пять 4) шесть
10.	При разработке политики ИБ необходимо руководствоваться следующим основным правилом: 1) команда разработчиков политики ИБ не должна превышать 20 человек 2) стоимость защиты конкретного актива не должна превышать стоимости самого актива 3) как следует реагировать на атаки вторжения 4) какую информацию следует регистрировать и прослеживать при функционировании системы защиты
11.	Архитектура безопасности включает как минимум следующее число компонентов: 1) два 2) три 3) четыре 4) пять
12.	В политике безопасности организации должны быть определены: 1) стандарты 2) правила безопасности 3) операции безопасности 4) процессы безопасности
13.	Каждое действие в процессе безопасности включает следующее число компонентов: 1) два 2) три 3) четыре 4) пять
14.	Каждое действие в процессе безопасности включает: 1) операцию 2) механизм 3) управление 4) выход
15.	Защищаемые ресурсы (данные, файлы, базы данных, программы) могут быть разделены на следующее число групп: 1) два 2) три 3) четыре 4) пять
16.	Компоненты архитектуры безопасности включают: 1) физическую безопасность 2) логическую безопасность 3) периметр безопасности сети 4) защиту ресурсов
17.	Административные полномочия подразделяются на следующее число категорий: 1) два 2) три 3) четыре 4) пять
18.	В основные задачи управления ИБ входят: 1) управление конфигурациями объектов и субъектов доступа; 2) управление доступом к базе данных 3) управление учетными записями и правами доступа к активным сетевым устройствам, рабочим станциям и серверам 4) управление конфигурациями объектов и субъектов доступа
19.	Последовательность процессов для обнаружения проблемы и выдачи сигнала тревоги включает следующее число шагов: 1) два 2) три 3) четыре 4) пять
20.	Подсистемы управления обновлениями позволяют автоматизировать следующие задачи: 1) возможность назначения обновлений определенным рабочим станциям и серверам или группам рабочих станций и серверов

<table>
<tr><td></td><td>2) контроль времени обновления ПО
3) автоматическое получение обновлений с сайтов производителей ПО
4) организацию централизованного хранилища обновлений</td></tr>
<tr><td>21.</td><td>Использование централизованного управления рабочими станциями и серверами позволяет:
1) создавать типовые образы рабочих станций и серверов
2) существенно сократить затраты на обеспечение актуальной конфигурации оборудования
3) распределять административные роли по типам и группам устройств
4) поддерживать соответствие локальных настроек политике безопасности организации</td></tr>
<tr><td></td><td>Выбрать несколько ответов</td></tr>
<tr><td>22.</td><td>Что входит в описание границ системы?
А) структура организации
Б) ресурсы информационной системы, подлежащие защите
В) технология обработки информации и решаемые задачи
Г) размещение средств СВТ и поддерживающей инфраструктуры</td></tr>
<tr><td>23.</td><td>Среди требований к режиму информационной безопасности следует отнести:
А) определить ценность ресурсов;
Б) к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;
В) рассчитать вероятности угроз;
Г) выявить уязвимости ресурсов;
Д) оценить потенциальный ущерб от воздействий злоумышленников.</td></tr>
<tr><td>24.</td><td>Среди подходов к управлению информационными рисками следует отнести:
А) уменьшение риска;
Б) уклонение от риска;
В) изменение характера риска;
Г) принятие риска.</td></tr>
<tr><td>25.</td><td>Технология управления режимом информационной безопасности в полном варианте содержит следующие элементы:
А) документирование информационной системы организации с позиции информационной безопасности;
Б) категорирование информационных ресурсов с позиции руководства организации;
В) определение возможного воздействия различного рода происшествий в области безопасности на информационную технологию;
Г) анализ рисков;
Д) технология управления рисками на всех этапах жизненного цикла;
Е) аудит в области информационной безопасности.</td></tr>
<tr><td>26.</td><td>Стандарт ISO содержит следующие разделы:
А) Часть 1. «Представление и общая модель».
Б) Часть 2. «Требования к функциям безопасности»
В) Часть 3. «Требования гарантированности безопасности»</td></tr>
<tr><td></td><td>Вопрос на сопоставление</td></tr>
<tr><td>27.</td><td>Сопоставьте этапы политики безопасности и их характеристики
<table>
<tr><td>1 этап</td><td>Выбор национальных и международных руководящих документов и стандартов в области ИБ</td></tr>
<tr><td>2 этап</td><td>Выработка подходов к управлению информационными рисками и принятие решения о выборе уровня защищенности КИС</td></tr>
<tr><td>3 этап</td><td>Структуризация контрмер по защите информации по следующим основным уровням: административному, процедурному, программно-техническому</td></tr>
<tr><td>4 этап</td><td>Установление порядка сертификации и аккредитации КИС на соответствие стандартам в сфере ИБ</td></tr>
</table></td></tr>
<tr><td></td><td>Расположение в правильном порядке</td></tr>
<tr><td>28.</td><td>Выстройте в правильном порядке этапы определения политики безопасности.
1 Выбор национальных и международных руководящих документов и стандартов в области ИБ
2 Выработка подходов к управлению информационными рисками и принятие решения о выборе уровня защищенности КИС
3 Структуризация контрмер по защите информации по следующим основным уровням: административному, процедурному, программно-техническому
4 Установление порядка сертификации и аккредитации КИС на соответствие стандартам в сфере ИБ</td></tr>
</table>

<table>
<tr><td></td><td>Вставить пропущенное слово или число</td></tr>
<tr><td>29.</td><td>Комплекс мероприятий по объективной идентификации и оценке наиболее важных для компании информационных процессов, степени их защищенности и контроля – это…(Управление информационными рисками)</td></tr>
<tr><td>30.</td><td>Организации описывают _____ нормативного соответствия и эффективности мер реагирования на риски, а также то, как контролируются _____, способные повлиять на эффективность реагирования на риски. (методы оценки , изменения)</td></tr>
<tr><td>31.</td><td>Документ NIST SP 800-37 ”Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy” («_____ управления рисками для информационных систем и организаций: жизненный цикл систем для обеспечения безопасности и конфиденциальности») (Фреймворк)</td></tr>
<tr><td></td><td>Задачи на 1-2 действия</td></tr>
<tr><td>32.</td><td>Опишите перечисленные ниже риски организации структурно по следующим характеристикам: опасность, подверженность риску, чувствительность к риску и степень взаимодействия рисков:
а) риск невыполнения обязательств со стороны поставщиков;
б) риск поломки производственной линии;
в) риск нереализации произведенной продукции.</td></tr>
<tr><td>33.</td><td>Отнесите каждый из перечисленных ниже рисков к одной из групп согласно их классификации по основным сферам (областям) деятельности организации:
1) риск аварии грузового судна во время перевозки груза, ожидаемого компанией;
2) риск резкого снижения курса рубля по отношению к доллару и евро для компании, осуществляющей экспортные операции;
3) риск возникновения сбоев в поставках сырья;
4) риск снижения спроса на продукцию предприятия;
5) риск отвержения рынком нового товара организации;
6) риск потери прибыли в результате снижения рыночных цен на товар;
7) риск просрочки выплаты долга дебитором;
8) риск разрушения складского помещения фирмы в результате стихийного бедствия;
9) риск поражения вирусом компьютерных сетей компании;
10) риск утечки информации, представляющей коммерческую тайну;
11) риск возникновения на рынке нового сильного конкурента;
12) риск потери платежеспособности;
13) риск поставки низкокачественных материалов поставщиком (с большой долей брака);
14) риск остановки производства в результате выхода из строя оборудования;
15) риск ухода с рынка основного промышленного потребителя продукции предприятия;
16) риск банкротства банка, обслуживающего организацию;
17) риск отказа инвестора от дальнейшего финансирования проекта в процессе его реализации;
18) риск ухода ведущих специалистов компании.</td></tr>
<tr><td>34.</td><td>От эксплуатации основного средства компания может получать в течение шести лет доход в размере 120 тыс. руб. в год. Остаточная стоимость данного основного средства через 6 лет будет равна 40 тыс. руб. Какую минимальную сумму должно получить предприятие от продажи этого основного средства, чтобы в случае вложения вырученных денег в банк под 12 % годовых на шесть лет иметь доход не ниже, чем результат от эксплуатации основного средства? Осуществите оценку уровня риска по итогам расчетов стоимости инвестиций при условии, что рыночная стоимость основного средства соответствующих параметров ниже требуемой величины на 10 %, а вероятность продажи основного средства по желаемой цене составляет 70 %.</td></tr>
<tr><td>35.</td><td>Оцените риски доходности при выборе инвестиционного проекта, рассчитав ожидаемые нормы доходности для двух альтернативных проектов А и Б и дисперсию, характеризующую колеблемость ожидаемого дохода. Возможные нормы доходности инвестиционных проектов А и Б находятся в зависимости от будущего состояния экономики. Данная зависимость отражена в табл.
Данные для расчета ожидаемой нормы доходности вариантов вложения капитала в проекты А и Б
<table>
<tr><th>Состояние экономики</th><th>Вероятность данного состояния</th><th>Возможные нормы доходности по проекту А, %</th><th>Возможные нормы доходности по проекту Б, %</th></tr>
<tr><td>Подъем</td><td>0,25</td><td>80</td><td>25</td></tr>
<tr><td>Норма</td><td>0,5</td><td>20</td><td>20</td></tr>
<tr><td>Спад</td><td>0,25</td><td>50</td><td>15</td></tr>
</table>
</td></tr>
<tr><td>36.</td><td>Оцените уровень финансового риска по инвестиционной операции, рассчитав среднеквадратическое отклонение и коэффициент вариации на основе следующих данных. На рассмотрение представлено два альтернативных инвестиционных проекта. Показатели вероятного инвестиционного дохода по ним представлены в табл. 6. Для удобства расчеты рекомендуется представить в табличной форме.</td></tr>
</table>

Распределение вероятности ожидаемых доходов по инвестиционным проектам

Возможные значения конъюнктуры инвестиционного рынка	Инвестиционный проект А		Инвестиционный проект Б	
	Расчетный доход, тыс. руб.	Значение вероятности	Расчетный доход, тыс. руб.	Значение вероятности
Высокая	700	0,2	900	0,25
Средняя	450	0,66	600	0,5
Низкая	300	0,22	250	0,25

Таблица 7

Расчет среднеквадратического отклонения и коэффициента вариации по инвестиционным проектам А и Б

Варианты проектов	Возможные значения конъюнктуры инвестиционного рынка	R_i	$\bar{R}$	$(R_i - \bar{R})^2$	P_i	$(R_i - \bar{R})^2 \cdot P_i$	$\sqrt{(R_i - \bar{R})^2} \cdot \sqrt{P_i}$	CV
Инвестиционный проект А	Высокая							
	Средняя							
	Низкая							
	В целом							

	Кейс-задания
37.	Требуется выявить наиболее значимые риски для конкретного вида предпринимательской деятельности. Для этого обучающиеся разрабатывают пример хозяйствующего субъекта. Желательно, чтобы это была реально действующая организация, но допускается и использование модели организации. Описание субъекта должно включать в себя следующие данные: 1) название организации; 2) виды деятельности; 3) масштаб деятельности (размер бизнеса); 4) регион, в котором работает субъект; 5) другие данные, которые обучающиеся посчитают необходимыми. На основе этих сведений группы составляют список всех возможных рисков, которым подвержен данный экономический субъект. Каждый риск оценивается сточки зрения вероятности его реализации и возможного ущерба. Берутся приблизительные значения этих показателей соответственно в процентах и в рублях. Кроме того, возможна оценка вероятности и ущерба по десятибалльной шкале. На данном этапе рекомендуется выявить не менее 15–20 рисков. На следующем этапе группа отсекает наименее вероятные риски, а также риски, связанные с незначительными потерями, т. е. все те риски, которые, по мнению обучающихся, не требуют каких-либо управляющих воздействий. На данном этапе рекомендуется оставить не более 10 рисков. Далее на основе идентифицированных рисков группа должна построить причинно-следственную диаграмму (диаграмму Исикавы). Результаты работы группы презентуются ее представителем в виде короткого доклада, а затем подвергаются обсуждению. После того, как докладчик окончит свое выступление, ему могут задаваться дополнительные вопросы представителями других групп, выступающими заинтересованными лицами. Каждый из них сам определяет свою роль, встает, представляется и задает вопрос. Отвечать на вопросы может как сам докладчик, так и его коллеги по группе.

3.2.1 *Шифр и наименование компетенции*

ПКв-4 Способность к разработке требований и проектированию программного обеспечения

№ задания	Тестовое задание
	Выбрать один ответ
1.	Основные задачи управления ИБ включают следующее их число: 1) два 2) три 3) четыре 4) пять
2.	Подсистемы управления обновлениями позволяют автоматизировать следующее число задач: 1) два 2) три 3) четыре 4) пять
3.	Централизованное управление сетевым оборудованием позволяет: 1) осуществлять мониторинг сетевых устройств 2) производить откат неудачных изменений конфигурации 3) поддерживать соответствие локальных настроек политике безопасности организации 4) централизованно хранить конфигурации активного сетевого оборудования

4.	Использование централизованного управления рабочими станциями и серверами позволяет удовлетворить следующее число требований: 1) два 2) три 3) четыре 4) пять
5.	Централизованное управление сетевым оборудованием позволяет удовлетворить следующее число требований: 1) два 2) три 3) четыре 4) пять
6.	GSM в сфере ИБ — это: 1) аналог системы ГЛОНАСС 2) концепция глобального управления безопасностью 3) узкоспециализированная система централизованного управления безопасностью 4) децентрализованная система управления безопасностью
7.	В GSM, как правило, используется: 1) матричный метод доступа 2) мандатное управление доступом 3) дискреционное управление доступом 4) избирательное управление доступом
8.	Задача ролевого разграничения доступа к конфигурационным командам реализуется инструментальными комплексами при выполнении следующих этапов: 1) сканирование активного сетевого оборудования 2) анализ полученных результатов и создание политики безопасности с целью разграничения доступа к конфигурационным командам 3) проверки данных учетной записи с целью установки соответствия пользователя множеству зарегистрированных субъектов доступа 4) создание конфигурации для ролевого разграничения доступа командам
9.	Группы, на которые могут быть разбиты правила глобальной политики безопасности включают: 1) правила пакетной фильтрации 2) правила VPN 3) правила, отвечающие за мониторинг инцидентов 4) прокси-правила
10.	GSM, ориентированная на управление безопасностью предприятия на принципах PBM, удовлетворяет следующему количеству требований: 1) два 2) три 3) четыре 4) пять
11.	Правила глобальной политики безопасности могут быть распространены как на: 1) сетевые взаимодействия 2) функции контроля системы 3) функции мониторинга системы 4) функции контроля и управления системы
12.	Объектами глобальной политики безопасности могут быть: 1) структурные подразделения компании 2) отдельная фирма 3) подразделение аудита фирмы 4) финансовый департамент
13.	В число политик безопасности входят: 1) стартовая политика безопасности устройства 2) политика реагирования на события 3) локальная политика безопасности 4) политика допустимого использования
14.	Величина риска R определяется на основе стоимости ресурса f, вероятности осуществления угрозы p и величины уязвимости u по следующей формуле: 1) $R = f /(p u)$ 2) $R = f p u$ 3) $R = f p/ u$

	4) R = (f/ p) u
15.	При реализации мандатной политики доступа: 1) все субъекты и объекты системы должны быть идентифицированы 2) права доступа субъекта к объекту системы определяются на основании некоторого правила 3) каждому объекту системы присваивается метка критичности 4) каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ
16.	Реализация методологии оценки рисков ИБ по NIST SP 800-30 включает следующее число основных шагов: 1) 8 2) 9 3) 10 4) 11
17.	Управление рисками в сфере ИБ реализуется на следующем уровне: 1) процедурном 2) административном 3) архитектурном 4) мандатном
18.	Обязательным условием начала разработки политики ИБ является: 1) наличие на фирме службы защиты информации 2) наличие на фирме функционирующей ИС 3) наличие на фирме высококвалифицированных специалистов в области защиты информации 4) возможность привлечения к разработке политики ИБ сторонних специалистов
19.	К специализированным политикам, затрагивающим значительное число пользователей, относятся: 1) политика защиты информации 2) политика удаленного доступа к ресурсам сети; 3) политика безопасности виртуальных защищенных сетей 4) политика допустимого использования
20.	Преимуществом мандатного метода управления доступом, используемого в соответствующей политике ИБ, является: 1) обеспечение более высокой надежности работы самой ИС 2) простота определения правил разграничения доступа 3) широкое распространение данного метода для работы с конфиденциальной информацией 4) предотвращение утечки информации из объектов с высокой меткой конфиденциальности в объекты с низкой меткой конфиденциальности
21.	Политика допустимого использования предназначается в основном для: 1) администраторов сети 2) администраторов безопасности 3) конечных пользователей 4) всех вышеуказанных сотрудников
	Выбрать несколько ответов
22.	В настоящее время наибольшую популярность получили следующие технологии, реализующие модель AAA: 1) RADIUS 2) TACACS 3) RADIUS 4) TACACS
23.	Каковы этапы модели LifeCyde Security? А) Политики безопасности, стандарты, процедуры и метрики Б) Анализ рисков В) Стратегический план построения системы защиты Г) Выбор и внедрение решений Д) Обучение персонала Е) Мониторинг защиты
24.	Случаи проведения анализа рисков ИС: А) обновления информационной системы или существенных изменений в ее структуре; Б) перехода на новые информационные технологии построения КИС; В) организации новых подключений в компании (например, подключения локальной сети

	филиала к сети головного офиса); Г) подключения к глобальным сетям (в первую очередь к Internet); Д) изменений в стратегии и тактике ведения бизнеса (например, при открытии электронного магазина); Е) проверки эффективности корпоративной системы защиты информации.
25.	Ключевыми моментами анализа информационных рисков КИС являются: А) подробное документирование и картирование системы, причем особое внимание необходимо уделять критически важным для бизнеса приложениям; Б) определение степени зависимости организации от штатного функционирования и структурных элементов системы, безопасности хранимых и обрабатываемых данных; В) обнаружение и учет уязвимых мест; Г) выявление и учет потенциальных угроз; Д) оценка и учет информационных рисков; Е) оценка потенциального ущерба собственникам информации и КИС в целом
26.	В плане подхода к обеспечению ИБ в АС можно выделить четыре группы отечественных заказчиков работ в области защиты информации: А) государственные структуры; Б) коммерческие структуры с формальными собственниками информационных ресурсов компании; В) коммерческие структуры с настоящими собственниками информационных ресурсов компании; Г) структуры, для которых обязательно соответствие зарубежным стандартам в области информационной безопасности.
27.	Угрозы по классам: А) форс-мажорные обстоятельства; Б) недостатки организационных мер; В) ошибки человека; Г) технические неисправности; Д) преднамеренные действия.
28.	Контрмеры по классам: А) улучшение инфраструктуры; Б) административные контрмеры; В) процедурные контрмеры; Г) программно-технические контрмеры; Д) уменьшение уязвимости коммуникаций; Е) планирование действий в чрезвычайных ситуациях.
	Вопрос на сопоставление
29.	Сопоставьте уровни зрелости компании и их признаки: 1Анархия — А) Сотрудники сами определяют, что хорошо, а что плохо; затраты и качество не прогнозируются 2Фольклор — Б) Выявлена определенная повторяемость организационных процессов 3Стандарты — В) Корпоративная мифология записана на бумаге; процессы повторяемы и не зависят от личных качеств исполнителей 4Измеряемый — Г) Процессы измеряемы и стандартизованы 5Оптимизируемый — Д) Фокус на повторяемости, измерении эффективности, оптимизации Вся информация о функционировании процессов фиксируется Ответ: 1-А, 2-Б, 3-В, 4-Г, 5-Д
30.	Сопоставьте фазу жизненного цикла информационной технологии фазе управления рисками 1. Предпроектная стадия (концепция данной ИС: определение целей и задач и их документирование) — А) Выявление основных классов рисков для данной ИС, вытекающих из целей и задач, концепция обеспечения ИБ 2. Проектирование ИС — Б) Выявление рисков, специфичных для данной ИС (вытекающих из особенностей архитектуры ИС) 3. Создание ИС: поставка элементов, монтаж, настройка и конфигурирование — В) До начала функционирования ИС должны быть идентифицированы и приняты во внимание все классы рисков 4. Функционирование ИС — Г) Периодическая переоценка рисков, связанная с изменениями внешних условий и в конфигурации ИС

	5. Прекращение функционирования ИС (информационные и вычислительные ресурсы более не используются по назначению и утилизируются — Д) Соблюдение требований информационной безопасности по отношению к выводимым информационным ресурсам Ответ: 1-А, 2-Б, 3-В, 4-Г, 5-Д
31.	Сопоставьте источник угрозы и результаты реализации угрозы 1. Хакер — А) Неавторизованный доступ к ИС с использованием известных уязвимостей ОС (описание сценария) 2. Криминальные структуры — Б) Проникновение в ИС с целью получить конфиденциальные данные (описание сценария) Ответ: 1-А, 2-Б
32.	Сопоставьте уровень и классы управляющих воздействий и критериев безопасности 1. Организационный уровень — А)разграничение ответственности; периодический пересмотр системы управления в области ИБ; протоколирование и разбор инцидентов в области ИБ; оценка рисков; обучение в области ИБ; процедура авторизации в ИС и удаления учетных записей; поддержание в актуальном состоянии плана обеспечения ИБ 2. Процедурный уровень — Б) Обеспечение правил поддержания режима ИБ 3. Программно-технический уровень — В) активный аудит и система реагирования; идентификация и аутентификация; криптографическая защита; реализация ролевой модели доступа; контроль за режимом работы сетевого оборудования Ответ: 1-А, 2-Б, 3-В
	Расположение в правильном порядке
33.	Расположите в правильном порядке методы технического уровня: 1) обеспечение требований базового уровня (идентификация, управление системой распределения ключей, администрирование, способы защиты элементов системы и ПО) 2) упреждающие меры (аутентификация, авторизация, обеспечение безотказности, контроль доступа, сохранение конфиденциальности транзакций 3) обнаружение нарушений в области ИБ и процедуры восстановления (аудит, выявление вторжений, антивирусная защита, проверка целостности ПО и данных) Ответ: 1, 2, 3
34.	Оценка информационных рисков компании может быть выполнена в соответствии со следующим планом (восстановите последовательность): 1) Идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса. 2) Оценивание возможных угроз. 3) Оценивание существующих уязвимостей. 4) Оценивание эффективности средств обеспечения информационной безопасности. Ответ: 1, 2, 3, 4
35.	Управление рисками предприятия в сфере информационной безопасности требует выполнения четырех этапов (восстановите последовательность): 1) Распознавание (идентификация) рисков. 2) Определение размера риска. 3) Разработка плана управления рисками. 4) Текущий контроль и управление рисками
	Вставить пропущенное слово или число
36.	Ожидаемые годовые потери, т.е. «стоимость» всех инцидентов за год (ALE)
37.	Методология _____ (Failure Modes and Effect Analysis) предлагает проведение оценки системы с точки зрения её слабых мест для поиска ненадежных элементов (FMEA)
38.	Методология _____ (Facilitated Risk Analysis Process) является относительно упрощенным способом оценки рисков, с фокусом только на самых критичных активах. Качественный анализ проводится с помощью экспертной оценки. (FRAP)
39.	Методология _____ (Operationally Critical Threat, Asset, and Vulnerability Evaluation) сфокусирована на самостоятельной работе членов бизнес-подразделений. Она используется для масштабной оценки всех информационных систем и бизнес-процессов компании. (OCTAVE)
	Задачи на 1-2 действия

40.	Выручка оператора информационных ресурсов составляет 900 тыс. ден. ед., переменные затраты – 200 тыс. ден. ед., постоянные затраты – 270 тыс. ден. ед. Необходимо определить запас финансовой прочности. Оценить на сколько процентов изменится прибыль предприятия, если эксперты оценивают снижения спроса на услуги оператора информационных ресурсов на 15%? Какой процент прибыли удастся сохранить предприятию, если выручка упадет на 40%? Каким должен быть процент снижения выручки, при котором оператор информационных ресурсов полностью лишится прибыли?
41.	Определить затраты на создание информационной системы, если время, затраченное на разработку системы, составляет 2,4 месяца, из них 2 месяца разработчик провел за компьютером. Оклад программиста 15000 руб. Среднегодовая норма рабочего времени 1986 часов. Затраты на материалы составляют 73000 руб., из них 65000 руб. потрачено на приобретение ПК и необходимого оборудования, суммарная мощность потребления электроэнергии которых 650 Вт. Цена электроэнергии 2,1 за 1 кВт/час.
42.	Составить перечень наиболее распространенных угроз информационной безопасности для данной организации. Выполнить анализ угроз и их последствий, определение слабостей в защите; провести оценку рисков, заполнив типичную форму для анализа рисков (таблица). Типичная форма для анализа рисков Пояснения к таблице: 1) В графе 1 содержится описание возможного риска, например: непреднамеренные ошибки пользователей – ввод неверных данных о клиентах. 2) В графе 2 описывается возможный результат, к которому может привести реализация риска, например: потеря клиента или штрафные санкции с его стороны. 3) В графе 3 описывается возможный результат в стоимостном выражении, т.е. что потеряет фирма в результате реализации возможного риска, например: 10000 руб. т.е. что потеряет фирма в результате реализации возможного риска, например: 10000 руб. или в виде оценок: 1 – низкая; 2 – средняя; 3 – высокая оценка стоимости последствий реализации риска. 4) В графе 4 задается вероятность осуществления данного риска. Для вероятности приняты следующие значения: высокая – 0,75; средняя – 0,5; низкая – 0,25; малая – 0,05 или в виде оценок: 1 – низкая; 2 – средняя; 3 – высокая оценка вероятности. 5) В графе 5 задается приоритет данного риска, который определяется как произведение вероятности на возможную стоимость риска и на 10-3 , например: 10000*0,25*10-3 = 2,5 или в виде оценки 2*3= 6 6) В графе 6 описываются предлагаемые меры защиты, которые представляют собой реализацию защитных мероприятий трех направлений пункта 6 применительно к вашей фирме, например: строгий контроль вводимых данных, обеспечиваемый программным способом; обучение персонала; ввод штрафных санкций за допущенные ошибки. 7) В графе 7 задается стоимость мер защиты, предлагаемых в графе 6, например, разработка дополнительного модуля контроля вводимых данных – 5000 руб.; обучение персонала на курсах – 30000 руб. Представление полученных результатов провести с использованием MS Excel.

3.2 Собеседование (вопросы для Экзамена)

3.2.1 *Шифр и наименование компетенции*

УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Номер вопроса	Текст вопроса
43.	Анализ информационных рисков предприятия
44.	Методы анализа данных при аудите ИБ
45.	Методы оценивания информационных рисков
46.	Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга)
47.	Гармонизированные критерии Европейских стран
48.	Германский стандарт BSI
49.	Британский стандарт BS 7799
50.	Международный стандарт ISO 17799
51.	Международный стандарт ISO 15408 «Общие критерии»
52.	Стандарт COBIT

3.2.2 *Шифр и наименование компетенции*

ПКв-4 Способность к разработке требований и проектированию программного обеспечения

Номер вопроса	Текст вопроса
1.	Стандарты по безопасности информационных технологий в России
2.	Методология оценки безопасности информационных технологий по ОК

3.	Оценка уровня доверия функциональной безопасности информационной технологии
4.	Назначение стандарта ISO 17799 для управления информационной безопасностью
5.	Практика прохождения аудита и получения сертификата ISO 17799
6.	Анализ видов используемых программных продуктов
7.	Система CRAMM 21. Система КОНДОР
8.	Сетевые сканеры
9.	Задачи и содержание работ при проведении аудита ИБ
10.	Подготовка предприятия к проведению аудита ИБ
11.	Планирование процедуры аудита ИБ

Критерии и шкалы оценки:

- оценка «зачтено» выставляется студенту, если он активно участвует в собеседовании и обсуждении, подготовил аргументы в пользу решения, предложил альтернативы, выслушивал мнения других;

- оценка «не зачтено», если студент выполнял роль наблюдателя, не внес вклада в собеседование и обсуждение.

3.3 Подготовка к практической работы

3.3.1 *Шифр и наименование компетенции*

УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Номер вопроса	Текст вопроса
1.	Определить ожидаемую прибыль по мероприятию А и по мероприятию Б, а также общую ожидаемую прибыль. Исходные данные. Имеется два варианта вложения капитала в мероприятие А и Б. От мероприятия А ожидается получение прибыли в сумме 15 тыс. р. с вероятностью 0,6. От мероприятия Б ожидается получение прибыли в сумме 20 тыс. р. с вероятностью 0,4.
2.	Предприятие специализируется на выпуске товаров народного потребления. Предприятие хочет оценить инвестиционное решение на следующий год, исходя из анализа экономической рентабельности, имевшей место на предприятии в предыдущие 10 лет (табл. 1.3). Таблица 1.3 Данные о среднем значении экономической рентабельности предприятия за 10 лет Рентабель- ность Годы 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 ЭР, % 10 15 9 15 17 18 11 18 14 24 Оценить вероятность ошибки прогноза экономической рентабельности на 2016 год (по коэффициенту вариации), учитывая, что вероятность ошибки велика при kВ ≥ 25 %.
3.	Выбрать наименее рискованный вариант выпуска продукции, если количество выпускаемых изделий по первому варианту 340 шт., по второму 300 шт., предполагаемая себестоимость единицы продукции по первому варианту 8,4 млн. руб., а по второму – 8,6 млн. руб. В случае нереализации продукции, предприятие недополучит прибыли по первому варианту на сумму 550 млн. руб., а по второму – на 720 млн. руб. Расходы по переделке продукции составят: по первому варианту 150 млн. руб., по второму – 100 млн. руб.

Критерии и шкалы оценки:

- оценка «зачтено» выставляется студенту, если домашнее задание является самостоятельным, оригинальным текстом, в котором прослеживается авторская позиция, продуманная система аргументов, а также наличествует обоснованные выводы; используются термины, понятия по дисциплине, в рамках которой выполняется работа; полностью соответствует выбранной теме, цели и задачам; текст домашнего задания логически выстроен, имеет четкую структуру; работа соответствует всем техническим требованиям; домашнее задание выполнено в установленный срок.

- оценка «не зачтено», выставляется студенту, если домашнее задание не является самостоятельным, оригинальным текстом, в котором не прослеживается авторская позиция, не продумана система аргументов, а также отсутствуют обоснованные выводы; не используются термины, понятия по дисциплине, в рамках которой выполняется работа; не соответствует выбранной теме, цели и задачам; текст домашнего задания композиционно не выстроен; работа не соответствует техническим требованиям; домашнее задание не выполнено в установленный срок.

3.3.1 *Шифр и наименование компетенции*

ПКв-4 Способность к разработке требований и проектированию программного обеспечения

Номер вопроса	Текст вопроса

1.	Определить ожидаемую прибыль по мероприятию А и по мероприятию Б, а также общую ожидаемую прибыль. Исходные данные. Имеется два варианта вложения капитала в мероприятие А и Б. От мероприятия А ожидается получение прибыли в сумме 15 тыс. р. с вероятностью 0,6. От мероприятия Б ожидается получение прибыли в сумме 20 тыс. р. с вероятностью 0,4.
2.	Предприятие специализируется на выпуске товаров народного потребления. Предприятие хочет оценить инвестиционное решение на следующий год, исходя из анализа экономической рентабельности, имевшей место на предприятии в предыдущие 10 лет (табл. 1.3). Таблица 1.3 Данные о среднем значении экономической рентабельности предприятия за 10 лет Рентабель- ность Годы 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 ЭР, % 10 15 9 15 17 18 11 18 14 24 Оценить вероятность ошибки прогноза экономической рентабельности на 2016 год (по коэффициенту вариации), учитывая, что вероятность ошибки велика при kВ ≥ 25 %.
3.	Выбрать наименее рискованный вариант выпуска продукции, если количество выпускаемых изделий по первому варианту 340 шт., по второму 300 шт., предполагаемая себестоимость единицы продукции по первому варианту 8,4 млн. руб., а по второму – 8,6 млн. руб. В случае нереализации продукции, предприятие недополучит прибыли по первому варианту на сумму 550 млн. руб., а по второму – на 720 млн. руб. Расходы по переделке продукции составят: по первому варианту 150 млн. руб., по второму – 100 млн. руб.

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

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03 Положение о курсовых экзаменах и экзаменах;
- П ВГУИТ 4.1.02 Положение о рейтинговой оценке текущей успеваемости.

Для оценки знаний, умений, навыков обучающихся по дисциплине применяется рейтинговая система. Итоговая оценка по дисциплине определяется на основании определения среднеарифметического значения баллов по каждому заданию.

Зачет по дисциплине выставляется в зачетную ведомость по результатам работы в семестре после выполнения всех видов учебной работы, предусмотренных рабочей программой дисциплины (с отметкой «зачтено») и получении по результатам тестирования по всем разделам дисциплины не менее 60 %.

5. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания для каждого результата обучения по дисциплине

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений					
Знает	основные законодательные и нормативно-правовые документы, основные этические ограничения, принятые в обществе, основные понятия, методы выработки принятия и обоснования решений задач в рамках поставленной цели методы выбора оптимального решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	Результаты тестирования	Обучающимся даны правильные ответы менее чем на 59,99 % всех тестовых вопросов	Неудовлетворительно	Не освоена / недостаточный
			Обучающимся даны правильные ответы на 60-74,99% всех тестовых вопросов	Удовлетворительно	Освоена / базовый
			Обучающимся даны правильные ответы на 75-84,99% всех тестовых вопросов	Хорошо	Освоена / повышенный
			Обучающимся даны правильные ответы на 85-100% всех тестовых вопросов	Отлично	Освоена / повышенный
		Собеседование (зачет / экзамен)	Обучающийся обладает частичными и разрозненными знаниями, только некоторые из которых может связывать между собой	Неудовлетворительно	Не освоена / недостаточный
			Обучающийся обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Удовлетворительно	Освоена / базовый
			Обучающийся обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Хорошо	Освоена / повышенный
			Обучающийся обладает системным взглядом на изучаемый объект	Отлично	Освоена / повышенный
Умеет	формулирует перечень взаимосвязанных задач, обеспечивающих достижение поставленной цели, в том числе с использованием сервисных возможностей соответствующих информационных (справочных правовых)	Отчет по практическим работам, реферат	Обучающийся не владеет умениями выполнения заданий; не демонстрирует умений, предусмотренных планируемыми результатами обучения	Неудовлетворительно	Не освоена / недостаточный
			Обучающийся испытывает затруднения при выполнении заданий по алгоритму; демонстрирует минимальный набор умений, предусмотренных планируемыми результатами обучения	Удовлетворительно	Освоена / базовый
			Обучающийся выполняет задания с использованием алгоритма решения, при выполнении допускает незначительные ошибки и неточности, формулирует выводы; демонстрирует умения, предусмотренные планируемыми результатами обучения	Хорошо	Освоена / повышенный

	систем определять ожидаемый результат решения задач и разрабатывает различные виды планов по реализации проектов учетом действующих правовых норм, имеющихся ресурсов и ограничений		Обучающийся выполняет задания, формируя алгоритм решения, при выполнении не допускает ошибок и неточностей, формулирует выводы; демонстрирует умения, предусмотренные планируемыми результатами обучения	Отлично	Освоена / повышенный
Владеет	навыками проектирования решения задачи, выбирая оптимальный способ ее решения : навыками оценки вероятных рисков и ограничений в выборе решения поставленных задач	КР	Обучающийся не владеет умениями выполнения заданий; не демонстрирует умений, предусмотренных планируемыми результатами обучения	Неудовлетвори тельно	Не освоена / недостаточный
			Обучающийся испытывает затруднения при выполнении заданий по алгоритму; демонстрирует минимальный набор умений, предусмотренных планируемыми результатами обучения	Удовлетворите льно	Освоена / базовый
			Обучающийся выполняет задания с использованием алгоритма решения, при выполнении допускает незначительные ошибки и неточности, формулирует выводы; демонстрирует умения, предусмотренные планируемыми результатами обучения	Хорошо	Освоена / повышенный
			Обучающийся выполняет задания, формируя алгоритм решения, при выполнении не допускает ошибок и неточностей, формулирует выводы; демонстрирует умения, предусмотренные планируемыми результатами обучения	Отлично	Освоена / повышенный

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ПКв-4 Способность к разработке требований и проектированию программного обеспечения					
Знает	модели процесса разработки программного обеспечения; основные принципы процесса разработки программного обеспечения; основные подходы к интегрированию программных модулей; виды и варианты интеграционных решений; современные технологии и инструменты интеграции; методы и способы идентификации сбоев и ошибок при интеграции приложений стандарты качества программной документации, основы организации инспектирования и верификации, встроенные и основные специализированные инструменты анализа качества программных продуктов, графические средства проектирования архитектуры программных продуктов модели, принципы, подходы процесса проектирования	Результаты тестирования	Обучающимся даны правильные ответы менее чем на 59,99 % всех тестовых вопросов	Неудовлетворительно	Не освоена / недостаточный
			Обучающимся даны правильные ответы на 60-74,99% всех тестовых вопросов	Удовлетворительно	Освоена / базовый
			Обучающимся даны правильные ответы на 75-84,99% всех тестовых вопросов	Хорошо	Освоена / повышенный
			Обучающимся даны правильные ответы на 85-100% всех тестовых вопросов	Отлично	Освоена / повышенный
		Собеседование (зачет / экзамен)	Обучающийся обладает частичными и разрозненными знаниями, только некоторые из которых может связывать между собой	Неудовлетворительно	Не освоена / недостаточный
			Обучающийся обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Удовлетворительно	Освоена / базовый
			Обучающийся обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Хорошо	Освоена / повышенный
			Обучающийся обладает системным взглядом на изучаемый объект	Отлично	Освоена / повышенный

	программного обеспечения, виды и варианты к интегрированию программных модулей, основные этапы разработки программного обеспечения, основные принципы технологии структурного и объектно-ориентированного программирования				
Умеет	анализировать проектную и техническую документацию; использовать специализированные графические средства построения и анализа архитектуры программных продуктов; организовывать заданную интеграцию модулей в программные средства на базе имеющейся архитектуры и автоматизации бизнес-процессов; определять источники и приемники данных разрабатывать тестовые пакеты и тестовые сценарии; выявлять ошибки в системных компонентах на основе спецификаций создавать программу по разработанному алгоритму как отдельный модуль, оформлять документацию на программное средство	Отчет по практическим работам, реферат	Обучающийся не владеет умениями выполнения заданий; не демонстрирует умений, предусмотренных планируемыми результатами обучения	Неудовлетворительно	Не освоена / недостаточный
			Обучающийся испытывает затруднения при выполнении заданий по алгоритму; демонстрирует минимальный набор умений, предусмотренных планируемыми результатами обучения	Удовлетворительно	Освоена / базовый
			Обучающийся выполняет задания с использованием алгоритма решения, при выполнении допускает незначительные ошибки и неточности, формулирует выводы; демонстрирует умения, предусмотренные планируемыми результатами обучения	Хорошо	Освоена / повышенный
			Обучающийся выполняет задания, формируя алгоритм решения, при выполнении не допускает ошибок и неточностей, формулирует выводы; демонстрирует умения, предусмотренные планируемыми результатами обучения	Отлично	Освоена / повышенный

Владеет	навыками разрабатывать и оформлять требования к программным модулям по предложенной документации навыками разработки тестовых наборов (пакетов) для программного модуля, разрабатывать тестовые сценарии программного средства, инспектировать разработанные программные модули на предмет соответствия стандартам кодирования : навыками разработки кода программного продукта на основе готовой спецификации на уровне модуля	Курсовая работа	Обучающийся не владеет умениями выполнения заданий; не демонстрирует умений, предусмотренных планируемыми результатами обучения	Неудовлетвори тельно	Не освоена / недостаточный
			Обучающийся испытывает затруднения при выполнении заданий по алгоритму; демонстрирует минимальный набор умений, предусмотренных планируемыми результатами обучения	Удовлетворите льно	Освоена / базовый
			Обучающийся выполняет задания с использованием алгоритма решения, при выполнении допускает незначительные ошибки и неточности, формулирует выводы; демонстрирует умения, предусмотренные планируемыми результатами обучения	Хорошо	Освоена / повышенный
			Обучающийся выполняет задания, формируя алгоритм решения, при выполнении не допускает ошибок и неточностей, формулирует выводы; демонстрирует умения, предусмотренные планируемыми результатами обучения	Отлично	Освоена / повышенный