Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Управление рисками

Образовательная программа: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Курс: 4, семестр : 7

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**7**
1	Всего зачетных единиц (кредитов)	5
2	Всего часов	180
3	Всего занятий в контактной форме, час.	90
4	Лекции, час.	36
5	Практические занятия, час.	36
6	Лабораторные занятия, час.	0
7	из них в активной и интерактивной форме, час.	0
8	Аттестация, час.	2
9	Консультации, час.	16
10	Самостоятельная работа, час.	90
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	Э

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.03.01 Информационная безопасность

ФГОС введен в действие приказом №1515 от 01.12.2016 г. , дата утверждения: 20.12.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, базовая

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.03.01 Информационная безопасность

Рабочая программа обсуждена на заседании кафедры

ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.т.н. Хиценко В. Е.

Заведующий кафедрой:

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

заведующий кафедрой Трушин В. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ПК.1** **способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; *в части следующих результатов обучения*:**
з1. знать используемые программные средства анализа и управления рисками
у1. уметь обоснованно выбирать программные средства автоматизации процессов управления рисками
***Компетенция ФГОС*: ПК.12 способность принимать участие в проведении экспериментальных исследований системы защиты информации; *в части следующих результатов обучения*:**
з1. знать основные международные стандарты и рекомендации по управлению информационными рисками
у1. уметь проводить классификацию критичных информационных ресурсов, анализ угроз и рисков автоматизированных систем
***Компетенция ФГОС*: ПК.4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; *в части следующих результатов обучения*:**
з1. знать методики анализа рисков, методы и средства управления информационными рисками
з3. знать основные угрозы безопасности информации и модели нарушителя в информационных системах
у1. уметь разрабатывать предложения по совершенствованию политики безопасности компании
у2. уметь разрабатывать корпоративную методику анализа рисков

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Управление рисками	
ПК.1.з1 знать используемые программные средства анализа и управления рисками	
1.знать используемые программные средства анализа и управления рисками	Лекции; Практические занятия
ПК.1.у1 уметь обоснованно выбирать программные средства автоматизации процессов управления рисками	
2.уметь обоснованно выбирать программные средства автоматизации процессов управления рисками	Лекции; Практические занятия; Самостоятельная работа
ПК.4.з1 знать методики анализа рисков, методы и средства управления информационными рисками	
3.знать методики анализа рисков, методы и средства управления информационными рисками	Лекции; Практические занятия
ПК.4.з3 знать основные угрозы безопасности информации и модели нарушителя в информационных системах	
4.знать основные угрозы безопасности информации и модели нарушителя в информационных системах	Лекции; Практические занятия; Самостоятельная работа
ПК.4.у1 уметь разрабатывать предложения по совершенствованию политики безопасности компании	
5.уметь разрабатывать предложения по совершенствованию политики безопасности компании	Лекции; Практические занятия
ПК.4.у2 уметь разрабатывать корпоративную методику анализа рисков	
6.уметь разрабатывать корпоративную методику анализа рисков	Лекции; Практические занятия; Самостоятельная работа
ПК.12.з1 знать основные международные стандарты и рекомендации по управлению информационными рисками	

7.знать основные международные стандарты и рекомендации по управлению информационными рисками	Лекции; Практические занятия; Самостоятельная работа
ПК.12.у1 уметь проводить классификацию критичных информационных ресурсов, анализ угроз и рисков автоматизированных систем	
8.уметь проводить классификацию критичных информационных ресурсов, анализ угроз и рисков автоматизированных систем	Лекции; Практические занятия; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Управление рисками информационной безопасности организации				
1. Актуальность проблемы управления информационной безопасностью организации. Место и роль процессов по управлению рисками в общей системе обеспечения информационной безопасности и защиты информационных ресурсов.	0	4	1	Составление конспекта лекций
2. Методологические основы управления рисками. Понятия и определения в области управления рисками. Управление рисками в основных международных стандартах информационной безопасности. Модель процессов управления информационными рисками.	0	4	2, 3	Составление конспекта лекций. Дискуссия
3. Стратегии анализа информационных рисков организации. Сравнительные методики и основные подходы к анализу рисков ИБ. Инструментальные средства анализа рисков.	0	4	3, 4	Составление конспекта лекций
4. Оценка рисков информационной безопасности. Менеджмент-решение. Активы ИС, риски, угрозы и уязвимости. Идентификация активов при анализе рисков ИС. Анализ угроз информационной безопасности организации. Анализ уязвимостей информационной инфраструктуры организации. Обработка рисков информационной безопасности.	0	6	4	Составление конспекта лекций
5. Планирование деятельности по управлению рисками ИБ.	0	4	4, 5	Составление конспекта лекций
Дидактическая единица: Основные положения теории и практики управления информационной безопасностью, связанные с разработкой и обслуживанием информационных систем				

6. Роль управления информационными рисками в политике информационной безопасности организации. Управление инцидентами информационной безопасности в организации. Организационные вопросы обеспечения информационной безопасности. Порядок разработки, структура и содержание политик ИБ. Управление информационными рисками на различных стадиях жизненного цикла ИТ.	0	6	4, 5, 6	Составление конспекта лекций
7. Реализация концепции управления информационными рисками на практике. Проработка тестов по анализу и оценке угроз, уязвимостей и информационных рисков организаций. Примерный анализ и моделирование событий и инцидентов информационной безопасности в различных организациях.	0	4	6, 7, 8	Составление конспекта лекций
8. Программные средства, используемые для анализа и управления рисками. Обзор, анализ и сравнение современных программных продуктов по анализу рисков: COBRA, CRAMM, RiskWatch, Buddy System, RA Software Tool, IBM Tivoli Risk Manager, Экспертная система "Авангард". Проблемы внедрения в России. Практические примеры оценки рисков в ИТ и в бизнесе.	0	4	6, 7, 8	Составление конспекта лекций

Таблица 3.2

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Управление рисками информационной безопасности организации				
1. Модель процессов управления информационными рисками.	0	4	1, 2	Изучение различных моделей процессов управления информационными рисками.
2. Анализ угроз информационной безопасности организации. Анализ уязвимостей информационной инфраструктуры организации.	0	8	4	Классификация и анализ угроз информационной безопасности организации. Анализ уязвимостей информационной инфраструктуры организации.
3. Планирование деятельности по управлению рисками ИБ.	0	8	3, 5	изучение подходов к планированию деятельности по управлению рисками ИБ.

Дидактическая единица: Основные положения теории и практики управления информационной безопасностью, связанные с разработкой и обслуживанием информационных систем				
4. Организационные вопросы обеспечения информационной безопасности.	0	8	7, 8	Организационные вопросы обеспечения информационной безопасности.
5. Управление информационными рисками на различных стадиях жизненного цикла ИТ.	0	8	6, 7	Изучение особенностей управления информационными рисками на различных стадиях жизненного цикла ИТ

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 7				
1	РГЗ	6, 7	33	5
, подробная информация приведена в приложении №3 : Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ В.И. Аверченков— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с.— Режим доступа: http://www.iprbookshop.ru/6991.html.— ЭБС «IPRbooks»				
2	Подготовка к занятиям	2, 4	30	4
, подробная информация приведена в приложении №1 : Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ В.И. Аверченков— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с.— Режим доступа: http://www.iprbookshop.ru/6991.html.— ЭБС «IPRbooks»				
3	Подготовка к аттестации	6, 7, 8	27	7
, подробная информация приведена в приложении №2 : Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ В.И. Аверченков— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с.— Режим доступа: http://www.iprbookshop.ru/6991.html.— ЭБС «IPRbooks»				

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail
Консультирование	e-mail

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Максимальный балл
Семестр: 7	

Практические занятия:	40
РГЗ:	20
Экзамен:	40

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля	
		Защита РГЗ	Экзамен
ПК.1	з1. знать используемые программные средства анализа и управления рисками	+	+
	у1. уметь обоснованно выбирать программные средства автоматизации процессов управления рисками		+
ПК.12	з1. знать основные международные стандарты и рекомендации по управлению информационными рисками	+	+
	у1. уметь проводить классификацию критичных информационных ресурсов, анализ угроз и рисков автоматизированных систем		+
ПК.4	з1. знать методики анализа рисков, методы и средства управления информационными рисками	+	+
	з3. знать основные угрозы безопасности информации и модели нарушителя в информационных системах		+
	у1. уметь разрабатывать предложения по совершенствованию политики безопасности компании		+
	у2. уметь разрабатывать корпоративную методику анализа рисков		+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Галатенко В. А. Основы информационной безопасности. Курс лекций : учебное пособие для вузов / В. А. Галатенко ; под ред. В. Б. Бетелина ; Интернет ун-т информ. технологий. - М., 2004. - 260 с. : ил.

2. Мамаева Л. Н. Управление рисками : учебное пособие / Л. Н. Мамаева. - М., 2012. - 255 с. : ил., табл.

Дополнительная литература

1. Чернова Г. В. Практика управления рисками на уровне предприятия : учебное пособие / Г. В. Чернова. - СПб., 2000. - 172 с.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ В.И. Аверченков— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 c.— Режим доступа: http://www.iprbookshop.ru/6991.html.— ЭБС «IPRbooks»

8.2 Специализированное программное обеспечение

1 Windows
2 Office

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Применяется для электронных презентаций лекционных и практических занятий; для электронных презентаций публичных выступлений студентов

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Управление рисками

Образовательная программа: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по **дисциплине** Управление рисками приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля РГЗ(Р).	**Промежуточная аттестация - экзамен,**
ПК.1/Э способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	з1. знать используемые программные средства анализа и управления рисками	Дидактическая единица: Управление рисками информационной безопасности организации .1 Актуальность проблемы управления информационной безопасностью организации. Место и роль процессов по управлению рисками в общей системе обеспечения информационной безопасности и защиты информационных ресурсов. .1 Модель процессов управления информационными рисками.	РГЗ, разделы 1,2	Экзамен, вопросы 10-19
ПК.1/Э	у1. уметь обоснованно выбирать программные средства автоматизации процессов управления рисками	Дидактическая единица: Управление рисками информационной безопасности организации .1 Модель процессов управления информационными рисками. .2 Методологические основы управления рисками. Понятия и определения в области управления рисками. Управление рисками в основных международных стандартах информационной безопасности. Модель процессов управления информационными рисками.	РГЗ, разделы 1, 2	Экзамен, вопросы 10-19
ПК.12/ЭИ способность принимать участие в проведении экспериментальных исследований системы защиты информации	з1. знать основные международные стандарты и рекомендации по управлению информационными рисками	Дидактическая единица: Основные положения теории и практики управления информационной безопасностью, связанные с разработкой и обслуживанием информационных систем .4 Организационные вопросы обеспечения информационной безопасности. .5 Управление информационными рисками на различных стадиях жизненного цикла ИТ. .7 Реализация концепции управления информационными рисками на практике. Проработка тестов по анализу и оценке угроз, уязвимостей и информационных рисков организаций. Примерный анализ и моделирование	РГЗ, разделы 1,2	Экзамен, вопросы 16-19

		событий и инцидентов информационной безопасности в различных организациях. .8 Программные средства, используемые для анализа и управления рисками. Обзор, анализ и сравнение современных программных продуктов по анализу рисков: COBRA, CRAMM, RiskWatch, Buddy System, RA Software Tool, IBM Tivoli Risk Manager, Экспертная система "Авангард". Проблемы внедрения в России. Практические примеры оценки рисков в ИТ и в бизнесе.		
ПК.12/ЭИ	у1. уметь проводить классификацию критичных информационных ресурсов, анализ угроз и рисков автоматизированны х систем	Дидактическая единица: Основные положения теории и практики управления информационной безопасностью, связанные с разработкой и обслуживанием информационных систем .4 Организационные вопросы обеспечения информационной безопасности. .7 Реализация концепции управления информационными рисками на практике. Проработка тестов по анализу и оценке угроз, уязвимостей и информационных рисков организаций. Примерный анализ и моделирование событий и инцидентов информационной безопасности в различных организациях. .8 Программные средства, используемые для анализа и управления рисками. Обзор, анализ и сравнение современных программных продуктов по анализу рисков: COBRA, CRAMM, RiskWatch, Buddy System, RA Software Tool, IBM Tivoli Risk Manager, Экспертная система "Авангард". Проблемы внедрения в России. Практические примеры оценки рисков в ИТ и в бизнесе.	РГЗ, раздел 2	Экзамен, вопросы 1-9
ПК.4/Э способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной	з1. знать методики анализа рисков, методы и средства управления информационными рисками	Дидактическая единица: Управление рисками информационной безопасности организации .2 Методологические основы управления рисками. Понятия и определения в области управления рисками. Управление рисками в основных международных стандартах информационной безопасности. Модель	РГЗ, раздел 1	Экзамен, вопросы 7-18

безопасности объекта защиты		процессов управления информационными рисками. .3 Планирование деятельности по управлению рисками ИБ. .3 Стратегии анализа информационных рисков организации. Сравнительные методики и основные подходы к анализу рисков ИБ. Инструментальные средства анализа рисков.		
ПК.4/Э	з3. знать основные угрозы безопасности информации и модели нарушителя в информационных системах	Дидактическая единица: Управление рисками информационной безопасности организации .2 Анализ угроз информационной безопасности организации. Анализ уязвимостей информационной инфраструктуры организации. .3 Стратегии анализа информационных рисков организации. Сравнительные методики и основные подходы к анализу рисков ИБ. Инструментальные средства анализа рисков. .4 Оценка рисков информационной безопасности. Менеджмент-решение. Активы ИС, риски, угрозы и уязвимости. Идентификация активов при анализе рисков ИС. Анализ угроз информационной безопасности организации. Анализ уязвимостей информационной инфраструктуры организации. Обработка рисков информационной безопасности. .5 Планирование деятельности по управлению рисками ИБ. .6 Роль управления информационными рисками в политике информационной безопасности организации. Управление инцидентами информационной безопасности в организации. Организационные вопросы обеспечения информационной безопасности. Порядок разработки, структура и содержание политик ИБ. Управление информационными рисками на различных стадиях жизненного цикла ИТ.	РГЗ , разделы 1, 2	Экзамен, вопросы 5-20
ПК.4/Э	у1. уметь разрабатывать предложения по совершенствованию политики безопасности компании	Дидактическая единица: Управление рисками информационной безопасности организации .3 Планирование деятельности по управлению рисками ИБ. .5 Планирование деятельности по управлению рисками ИБ.	РГЗ, раздел 2	Экзамен, вопросы 12-20

		.6 Роль управления информационными рисками в политике информационной безопасности организации. Управление инцидентами информационной безопасности в организации. Организационные вопросы обеспечения информационной безопасности. Порядок разработки, структура и содержание политик ИБ. Управление информационными рисками на различных стадиях жизненного цикла ИТ.		
ПК.4/Э	у2. уметь разрабатывать корпоративную методику анализа рисков	Дидактическая единица: Основные положения теории и практики управления информационной безопасностью, связанные с разработкой и обслуживанием информационных систем .5 Управление информационными рисками на различных стадиях жизненного цикла ИТ. .6 Роль управления информационными рисками в политике информационной безопасности организации. Управление инцидентами информационной безопасности в организации. Организационные вопросы обеспечения информационной безопасности. Порядок разработки, структура и содержание политик ИБ. Управление информационными рисками на различных стадиях жизненного цикла ИТ. .7 Реализация концепции управления информационными рисками на практике. Проработка тестов по анализу и оценке угроз, уязвимостей и информационных рисков организаций. Примерный анализ и моделирование событий и инцидентов информационной безопасности в различных организациях. .8 Программные средства, используемые для анализа и управления рисками. Обзор, анализ и сравнение современных программных продуктов по анализу рисков: COBRA, CRAMM, RiskWatch, Buddy System, RA Software Tool, IBM Tivoli Risk Manager, Экспертная система "Авангард". Проблемы внедрения в России.	РГЗ, раздел 2	Экзамен, вопросы 10-15

		Практические примеры оценки рисков в ИТ и в бизнесе.		

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 7 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ПК.1/Э, ПК.12/ЭИ, ПК.4/Э.

Экзамен проводится в устной форме и подразумевает ответы на два вопроса из разных разделов курса.

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 7 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе учебной дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ПК.1/Э, ПК.12/ЭИ, ПК.4/Э, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт экзамена

по дисциплине «Управление рисками», 7 семестр

1. Методика оценки

Экзамен проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов __1__, второй вопрос из диапазона вопросов __2__ (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к экзамену по дисциплине «Управление рисками»

---

1. Классификация информационных рисков.
2. Программные средства управления рисками базового уровня

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

2. Критерии оценки

- Ответ на экзаменационный билет (тест) считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *__5_ баллов.*
- Ответ на экзаменационный билет (тест) засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, вычислительные, оценка составляет *__10_ баллов.*
- Ответ на экзаменационный билет (тест) билет засчитывается на **базовом** уровне, если

студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *_30_ баллов.*

- Ответ на экзаменационный билет (тест) билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет _40_ *баллов.*

3. Шкала оценки

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к экзамену по дисциплине «**Управление рисками**»**

Диапазон 1

1.Сущность понятий «неопределенность» и «риск».
2. Элементы и функции риска.
3. Классификация рисков.
4. Понятие и особенности информационных рисков.
5. Виды информационных угроз и соответствующие бизнес-риски
6. Классификация информационных рисков.
7. Процесс анализа информационных рисков.
8. Источники возникновения информационных рисков.
9. Идентификация информационных рисков: особенности.
10. Методы оценки информационных рисков.

Диапазон 2

11. Измерение рисков: критерии, формулы, допустимый уровень риска.
12. Характеристика зарубежных стандартов управления информационными рисками.
13. Методики управления информационными рисками.
14. Особенности управления информационными рисками в России.
15. Методики управления информационными рисками.
16.Стандарты управления информационными рисками
17.Инструменты управления информационными рисками
18. Аудит безопасности
19. Программные средства управления рисками базового уровня.
20. Системы полного анализа риска.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт
расчетно-графического задания (работы)

по дисциплине «Управление рисками», 7 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны провести анализ уязвимостей, угроз и рисков информационной безопасности для заданного предприятия с использованием изученных методик, сравнительный анализ результатов и сделать вывод о предпочтительности методики для предприятия. В качестве объекта исследования может выступать организация, где проходила практика, или в которой будет выполняться выпускная квалификационная работа.

Обязательные структурные части РГЗ.

Введение (актуальность, цель, задачи)

1. Анализ объекта исследования
   - Основная деятельность организации
   - Организационная структура
   - Нормативно-правовая база, регламентирующая работу организации
   - Активы (в т.ч. информационные)
   - Схема потоков данных, описание информационных систем
2. Практическая часть
   - Анализ угроз и рисков с использованием разных методик
   - Сравнение результатов
3. Заключение

Оцениваемые позиции:

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), отсутствует анализ объекта, диагностические признаки не обоснованы, аппаратные и программные средства не выбраны или не соответствуют современным требованиям, оценка составляет __3___ балла.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы, аппаратные и программные средства не соответствуют современным требованиям, оценка составляет _7____ баллов.
- Работа считается выполненной **на базовом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны ,но не оптимизированы, аппаратные и программные средства выбраны без достаточного обоснования, оценка составляет _10____ баллов.
- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны и оптимизированы, выбор аппаратных и программных средств обоснован, оценка составляет __20___ баллов.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ(Р) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Примерный перечень методик анализа угроз и рисков при выполнении РГЗ(Р)**
    a) Анализ угроз и рисков с использованием вероятностной модели
    b) Анализ угроз и рисков с использованием методики «Microsoft Security Assessment Tool»
    c) Анализ угроз и рисков с использованием методики vsRisk
    d) Анализ угроз и рисков с использованием методики Practical Threat Analysis
    e) Анализ угроз и рисков с использованием методики Microsoft (The Security Risk Management Guide)