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
Аттестация и аудит информационной безопасности

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.	99
4	Лекции, час.	36
5	Практические занятия, час.	36
6	Лабораторные занятия, час.	0
7	из них в активной и интерактивной форме, час.	36
8	Аттестация, час.	2
9	Консультации, час.	25
10	Самостоятельная работа, час.	81
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	ДЗ

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:

старший преподаватель, Дронова Г. А.

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.13** **способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации; *в части следующих результатов обучения*:**
у2. уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных 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*:**
з4. знать принципы формирования политики информационной безопасности на объекте защиты
у4. уметь разрабатывать частные политики информационной безопасности информационных систем
***Компетенция ФГОС*: ПК.5 способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации; *в части следующих результатов обучения*:**
з3. знать порядок проведения аттестации объектов информатизации по требованиям безопасности информации
у2. уметь разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Аттестация и аудит информационной безопасности	
ПК.4.з4 знать принципы формирования политики информационной безопасности на объекте защиты	
1.знать принципы формирования политики информационной безопасности на объекте защиты	Лекции; Практические занятия; Самостоятельная работа
ПК.4.у4 уметь разрабатывать частные политики информационной безопасности информационных систем	
2.уметь разрабатывать частные политики информационной безопасности информационных систем	Лекции; Практические занятия; Самостоятельная работа
ПК.5.з3 знать порядок проведения аттестации объектов информатизации по требованиям безопасности информации	
3.знать порядок проведения аттестации объектов информатизации по требованиям безопасности информации	Лекции; Практические занятия; Самостоятельная работа
ПК.5.у2 уметь разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации	
4.уметь разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации	Лекции; Практические занятия; Самостоятельная работа
ПК.13.у2 уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем	
5.уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных 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
Семестр: 7			
Дидактическая единица: Современная ИТ-инфраструктура организации.			
1. Современная ИТ-инфраструктура организации. ИТ-объекты. Информационные ресурсы (активы) организации. Видовая классификация ресурсов.	0	6	1, 2
Дидактическая единица: Обеспечение информационной безопасности как бизнес-процесс			
2. Обеспечение информационной безопасности как бизнес-процесс. Дерево целей, дерево бизнес-функций. Концепция контроллинга и функционально-стоимостной анализ.	0	4	
3. Административная, функциональная подчиненность офицера по информационной безопасности (CISO). Ключевые показатели эффективности (KPI) CISO. Особенности взаимодействия CISO с бизнес-подразделениями.	0	4	
Дидактическая единица: Понятия аудита, аттестации, консалтинга и аутсорсинга в области информационной безопасности			
5. Понятия аудита, аттестации, консалтинга и аутсорсинга в области информационной безопасности. Аттестация объектов информатизации.	0	4	3, 4
6. ИТ-аудит и аудит информационной безопасности. Цели (Scope) и задачи проведения аттестации, аудита. Виды аудита.	0	4	
Дидактическая единица: Нормативная база, используемая при проведении аттестации, аудита ИБ			
7. Нормативная база, используемая при проведении аттестации, аудита ИБ. "Положение по аттестации объектов информатизации" Гостехкомиссии России. СТО БР ИББС-1.0-2010.	0	2	4
8. "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения". CobiT 4.1. "Framework. Control Objectives. Management Guidelines. Maturity Model".	0	2	
9. Международный стандарт ISO/IEC 27001:2005 Information technology-Security techniques-Information security management systems-Requirements. Процессионная модель "Plan-Do-Check-Act".	0	2	
Дидактическая единица: Планирование аудита информационной безопасности организации. Управление процессом аудита			
10. Особенности аудита информационной безопасности в РФ. Этические правила работы аудитора.	0	2	
11. Планирование аудита информационной безопасности организации. Управление процессом аудита.	0	2	
12. Практические этапы аудита. Методы, способы проведения аудита.	0	2	5
13. Экспертно-аналитический, инструментальный методы аудита. Виды отчетных документов по результатам проведения аудита.	0	2	5

Таблица 3.2

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Обеспечение информационной безопасности как бизнес-процесс				
2. Комплекс организационно-технических требований обеспечения безопасности информационных ресурсов	12	12	2, 4, 5	Разработка комплекса организационно-технических требований обеспечения безопасности информационных ресурсов компании на основе NIST Special Publication 800-53. Recommended Security Controls for Federal Information Systems.
Дидактическая единица: Нормативная база, используемая при проведении аттестации, аудита ИБ				
3. Методики аудита информационной безопасности организации	12	12	2, 3, 4	Разработка методики аудита информационной безопасности организации по отдельным группам контролей согласно ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности системы менеджмента информационной безопасности"
Дидактическая единица: Планирование аудита информационной безопасности организации. Управление процессом аудита				
1. "Информационная технология. Практические правила управления информационной безопасностью".	12	12	1, 2, 3, 4	Изучается разработка концепции, определяющей подсистемы системы менеджмента информационной безопасности компании в соответствии с ГОСТ Р ИСО/МЭК 17799-2005

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 7				
1	РГЗ	2, 3, 4	50	14
Выполнение РГЗ, подробная информация приведена в приложении №3 : Линник С. Е. Противодействия атакам на популярные сетевые сервисы : учебно-методическое пособие / С. Е. Линник, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2015. - 55, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000222748 Дронова Г. А. Аттестация и аудит информационной безопасности : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 14, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234014				
2	Подготовка к занятиям	1, 2, 4	20	4
Самостоятельная подготовка к занятиям: Дронова Г. А. Аттестация и аудит информационной безопасности : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 14, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234014				

3	Подготовка к аттестации	1, 2, 3, 4, 5	11	7
Самостоятельная подготовка к зачету, подробная информация приведена в приложении №2 : Моделирование и прогнозирование количества инцидентов в системе информационной безопасности при помощи динамической модели : методические указания к выполнению лабораторных работ по специальностям 090105 - Комплексное обеспечение информационной безопасности автоматизированных систем и 090104 - Комплексная защита объектов информатизации / Новосиб. гос. техн. ун-т ; [сост.: А. Ж. Абденов, Р. Н. Заркумова]. - Новосибирск, 2012. - 26 с. : табл., ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000173267 Дронова Г. А. Аттестация и аудит информационной безопасности : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 14, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234014 Анализ состояния защиты данных в информационных системах : учебно-методическое пособие / Новосиб. гос. техн. ун-т ; [сост. В. В. Денисов]. - Новосибирск, 2012. - 51, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000171050			

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; Портал НГТУ
Консультирование	e-mail
Размещение учебных материалов	ЭБС

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	Мин. балл	Максимальный балл
Семестр: 7		
РГЗ:	20	50
Контролирующие материалы (список вопросов) приводятся в "Дронова Г. А. Аттестация и аудит информационной безопасности : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 14, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234014"		
Зачет:	20	50
Контролирующие материалы (список вопросов) приводятся в "Дронова Г. А. Аттестация и аудит информационной безопасности : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 14, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234014"		

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	Зачет
ПК.13	у2. уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем	+	+

ПК.4	з4. знать принципы формирования политики информационной безопасности на объекте защиты	+	+
	у4. уметь разрабатывать частные политики информационной безопасности информационных систем	+	+
ПК.5	з3. знать порядок проведения аттестации объектов информатизации по требованиям безопасности информации	+	+
	у2. уметь разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации	+	+

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

7. Литература

Основная литература

1. Мельников В. П. Информационная безопасность и защита информации : учебное пособие для вузов по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М., 2008. - 330, [1] с. : ил., табл.

2. Грибунин В. Г. Комплексная система защиты информации на предприятии : [учебное пособие для вузов по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информации" направления подготовки "Информационная безопасность"] / В. Г. Грибунин, В. В. Чудовский. - М., 2009. - 411, [1] с. : ил., табл.

Дополнительная литература

1. Потемкин С. А. Концепция организационно-управленческого аудита / С. А. Потемкин, Т. А. Ларина // Деньги и кредит. - 2015. - № 5. - С. 55-62.

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. Дронова Г. А. Аттестация и аудит информационной безопасности : учебно-методическое пособие / Г. А. Дронова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 14, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234014

2. Моделирование и прогнозирование количества инцидентов в системе информационной безопасности при помощи динамической модели : методические указания к выполнению лабораторных работ по специальностям 090105 - Комплексное обеспечение информационной безопасности автоматизированных систем и 090104 - Комплексная защита объектов информатизации / Новосиб. гос. техн. ун-т ; [сост.: А. Ж. Абденов, Р. Н. Заркумова]. - Новосибирск, 2012. - 26 с. : табл., ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000173267

3. Анализ состояния защиты данных в информационных системах : учебно-методическое пособие / Новосиб. гос. техн. ун-т ; [сост. В. В. Денисов]. - Новосибирск, 2012. - 51, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000171050

4. Линник С. Е. Противодействия атакам на популярные сетевые сервисы : учебно-методическое пособие / С. Е. Линник, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2015. - 55, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000222748

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)	Для демонстрации основных положений курса

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

Аттестация и аудит информационной безопасности

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 Аттестация и аудит информационной безопасности приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ПК.13/ОУ способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	у2. уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем	Комплекс организационно-технических требований обеспечения безопасности информационных ресурсов Экспертно-аналитический, инструментальный методы аудита. Виды отчетных документов по результатам проведения аудита.	РГЗ, Разделы 1.1, 1.2	Зачет, Вопросы 1.1-1.5, 2.3-2.6
ПК.4/Э способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	з4. знать принципы формирования политики информационной безопасности на объекте защиты	"Информационная технология. Практические правила управления информационной безопасностью". Современная ИТ-инфраструктура организации. ИТ-объекты. Информационные ресурсы (активы) организации. Видовая классификация ресурсов.	РГЗ, Разделы 1.1, 1.2	Зачет, Вопросы 1.1-1.5, 2.1-2.2, 2.7-2.10
ПК.4/Э	у4. уметь разрабатывать частные политики информационной безопасности информационных систем	"Информационная технология. Практические правила управления информационной безопасностью". Комплекс организационно-технических требований обеспечения безопасности информационных ресурсов Методики аудита информационной безопасности организации Современная ИТ-инфраструктура организации. ИТ-объекты. Информационные ресурсы (активы) организации. Видовая классификация ресурсов.	РГЗ, Разделы 1.1, 1.2	Зачет, Вопросы 1.1-1.5, 2.3-2.6
ПК.5/Э способность принимать участие в организации и сопровождении аттестации объекта информатизации по	з3. знать порядок проведения аттестации объектов информатизации по требованиям безопасности	"Информационная технология. Практические правила управления информационной безопасностью". Методики аудита информационной безопасности организации	РГЗ, Разделы 1.1, 1.2	Зачет, Вопросы 1.1-1.5, 2.3-2.6

требованиям безопасности информации	информации	Понятия аудита, аттестации, консалтинга и аутсорсинга в области информационной безопасности. Аттестация объектов информатизации.		
ПК.5/Э	у2. уметь разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации	Нормативная база, используемая при проведении аттестации, аудита ИБ. "Положение по аттестации объектов информатизации" Гостехкомиссии России. СТО БР ИББС-1.0-2010.	РГЗ, Разделы 1.1, 1.2	Зачет, Вопросы 1.1-1.5, 2.3-2.6

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 7 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ПК.13/ОУ, ПК.4/Э, ПК.5/Э. Зачет проводится в устной форме, по билетам.

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

В 7 семестре обязательным этапом текущей аттестации являются 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 дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций, ПК.13/ОУ, ПК.4/Э, ПК.5/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 зачета

по дисциплине «Аттестация и аудит информационной безопасности», 7 семестр

1. Методика оценки

Зачет 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 билета для зачета

НОВОСИБИРСКИЙГОСУДАРСТВЕННЫЙТЕХНИЧЕСКИЙУНИВЕРСИТЕТ
Факультет АВТФ

Билет №_____
к зачетупо дисциплине «Аттестация и аудит информационной безопасности»

---

1. Вопрос 1
2. Вопрос 2.

Утверждаю: зав. кафедрой ____должность, ФИО
(подпись)
(дата)

2. Критерии оценки

- Ответ на билет для зачета считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать понимания основных рабочих процессов.
  Оценка составляет __*0*__ *баллов.*
- Ответ на билет для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, однако при описании процессов допускает ошибки.
  Оценка составляет __*30*__ *баллов.*
- Ответ на билет для зачета билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, показывает знание источников требований, дает характеристику и понимание процессов, однако не может провести анализ требований и представить качественные характеристики процессов.
  Оценка составляет _*70*__ *баллов.*
- Ответ на билет для зачета билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы формулирует основные понятия, показывает знание

источников требований, дает характеристику и понимание процессов, может провести анализ требований, может представить качественные характеристики процессов.

Оценка составляет _100_ *баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее _30__ баллов (из_100__возможных).

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

4. Вопросы к зачету по дисциплине «Аттестация и аудит информационной безопасности»

Диапазон 1 (значимость – 70%)

1. Применение ГОСТ Р ИСО/МЭК 27002 в аудите
2. Применение ГОСТ Р ИСО/МЭК 15408 в аудите
3. Применение СТО БС ИББС в аудите
4. Организационно-технические требования обеспечения безопасности. Аналитические методы и технические системы поиска уязвимостей. Оценка рисков
5. Планирование процесса аудита ИБ. Управление процессом аудита. Практические этапы аудита. Методы, способы проведения аудита.

Диапазон 2 (значимость – 30%)

1. Понятия аттестации, сертификации и аудита ИБ
2. Процесс ИБ. Аудит и подконтрольность
3. Категорирование и классификация информационных ресурсов организации
4. Понятие контролей. Цель и меры контроля
5. Процессы. Составляющие. Уровень зрелости процессов
6. Аудит и мониторинг ключевых показателей процессов
7. Нормативные документы, используемые при аудите, аттестации и сертификации
8. Понятие SLA. SLA в ИБ. Назначение, аудит
9. Понятие OLA. OLA в ИБ. Назначение, аудит
10. Понятие UC. UC в ИБ. Назначение, аудит

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

Паспорт
расчетно-графического задания (работы)

по дисциплине «Аттестация и аудит информационной безопасности», 7 семестр

1. **Методика оценки**

При выполнении расчетно-графического задания (работы) студенты должны разработать контрольную форму в политику аудита системы управления ИБ организации.

Обязательные структурные части РГЗ.

1. Контрольная форма по выбранной тематике аудита.
2. Перечень использованных нормативных документов.

Оцениваемые позиции:

1. Полезность контрольной формы.
2. Эффективность контрольной формы.
3. Перечень использованных документов.

2. **Критерии оценки**

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы не показывает знаний целей и методов аудита, не понимает сути процесса аудита, деятельности офицера безопасности.
  Оценка составляет _0_ *баллов.*
- Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы показывает понимание целей аудита, знание технических систем контроля, деятельности офицера безопасности, но слабо ориентируется в организации процесса, методах и средствах аудита.
  Оценка составляет __30__ *баллов.*
- Ответ на экзаменационный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы показывает понимание целей аудита, знание методов и средств аудита, технических систем контроля, деятельности офицера безопасности.
  Оценка составляет __50__ *баллов.*
- Ответ на экзаменационный билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы показывает понимание целей аудита, назначение мониторинга, знание методов и средств аудита, технических систем контроля, деятельности офицера безопасности, показывает умение формировать контрольные формы аудита.
- Оценка составляет _70_ *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 тем РГЗ(Р)**

1 Аудит процесса "Обеспечение физической безопасности и защита от воздействия окружающей среды" (подтема – ЦОД).

2 Аудит процесса "Осведомленность и информирование персонала".
3 Аудит процесса "Контроль логического доступа" (подтема – доступ в сеть).
4 Аудит процесса "Системная и информационная целостность" (подтема – защита от вредоносного кода).
5 Аудит процесса "Защита систем и связи" (подтема – криптографическая защита).