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
Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Курс: 4, семестр : 8

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**8**
1	Всего зачетных единиц (кредитов)	6
2	Всего часов	216
3	Всего занятий в контактной форме, час.	91
4	Лекции, час.	36
5	Практические занятия, час.	36
6	Лабораторные занятия, час.	0
7	из них в активной и интерактивной форме, час.	18
8	Аттестация, час.	2
9	Консультации, час.	17
10	Самостоятельная работа, час.	125
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): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС введен в действие приказом №1509 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): 10.05.03 Информационная безопасность автоматизированных систем

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, Туманов С. 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.17 способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации; *в части следующих результатов обучения*:**
з1. знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
у2. уметь проводить инструментальный мониторинг защищенности автоматизированных систем
***Компетенция ФГОС*: ПК.24 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности; *в части следующих результатов обучения*:**
у1. уметь выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем
***Компетенция ФГОС*: ПК.27 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы; *в части следующих результатов обучения*:**
з1. знать методы и средства проведения аудита и мониторинга безопасности информационных систем
***Компетенция ФГОС*: ПСК.35 способность проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов; *в части следующих результатов обучения*:**
у2. уметь внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей	
ПК.17.з1 знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	
1.Принципы разработки и эксплуатация систем мониторинга информационной безопасности и защиты компьютерных сетей.	Лекции; Самостоятельная работа
ПК.17.у2 уметь проводить инструментальный мониторинг защищенности автоматизированных систем	
2.Реализовать концепции разработки и эксплуатация систем мониторинга информационной безопасности компьютерных сетей.	Лекции; Самостоятельная работа
ПК.24.у1 уметь выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем	
3.Реализовать требования к системам мониторинга информационной безопасности АСЗИ.	Лекции; Самостоятельная работа
ПК.27.з1 знать методы и средства проведения аудита и мониторинга безопасности информационных систем	
4.Основные задачи организации функционирования и эксплуатация систем мониторинга информационной безопасности .	Лекции
ПСК.35.у2 уметь внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах	
5.Применять знания о системах мониторинга информационной безопасности	Практические занятия; Самостоятельная работа

6.Анализировать тенденции развития систем и средствмониторинга АСЗИ.	Практические занятия; Самостоятельная работа
7.Навыками анализа основных характеристик и возможностей систем мониторинга информационной безопасности АСЗИ.	Практические занятия

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 8				
Дидактическая единица: Предмет и задачи курса.				
1. Цели и задачи управление безопасностью информационной инфраструктурой.	1	2	1	Цели и задачи
Дидактическая единица: Принципы организации и этапы разработки				
2. Принципы организации и этапы разработки систем мониторинга информационной безопасности АСЗИ.	1	2	1, 2	Этапы разработки систем мониторинга АСЗИ
3. Дестабилизирующие воздействия на защищённые компьютерные сети и их нейтрализация.	2	4	1, 2, 3	Дестабилизирующие воздействия.
4. Задачи, решаемые при проведении анализа скрытых каналов и порядок проведения анализа скрытых каналов для продуктов и систем ИТ и АС	1	2	1, 2, 3, 4	ГОСТ Р 53113.1-2008
5. Определение возможностей несанкционированного доступа к защищаемой информации	1	2	2, 3	НСД
6. Определение компонентов систем мониторинга информационной безопасности АСЗИ	1	2	3, 4	Определение компонентов систем мониторинга информационной безопасности
7. Определение условий функционирования систем мониторинга информационной безопасности АСЗИ	1	2	1, 4	Определение условий функционирования
Дидактическая единица: Модели систем мониторинга АСЗИ				
8. Разработка модели систем мониторинга информационной безопасности АСЗИ.	2	4	1, 2	Разработка модели систем мониторинга
Дидактическая единица: Технологическое и организационное обеспечение				
9. Технологическое и организационное обеспечение построения систем мониторинга информационной безопасности АСЗИ.	2	4	3, 4	Технологическое и организационное обеспечение построения систем мониторинга
10. Принципы и методы планирования функционирования систем мониторинга информационной безопасности АСЗИ	2	4	3, 4	Методы планирования функционирования систем мониторинга.

11. Состав и содержание контроля функционирования систем мониторинга информационной безопасности АСЗИ.	2	4	3, 4	Состав и содержание контроля функционирования систем мониторинга .
Дидактическая единица: Методы и модели оценки эффективности систем мониторинга				
12. Методы и модели оценки эффективности систем мониторинга информационной безопасности АСЗИ.	2	4	2, 3	Методы и модели оценки эффективности систем мониторинга информационной безопасности

Таблица 3.2

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 8				
Дидактическая единица: Принципы организации и этапы разработки				
1. Разработка политики безопасности и регламента мониторинга	0	8	5, 6	Разработка политики безопасности и регламента мониторинга
2. Система управления информационной безопасностью предприятия.	0	4	5, 6, 7	Система управления информационной безопасностью предприятия.
3. Методы решения задач мониторинга информационной безопасности	0	8	6, 7	методы решения задач мониторинга информационной безопасности
4. Методика выявления состава систем мониторинга информационной безопасности	0	4	5, 6	Методика выявления состава систем мониторинга
Дидактическая единица: Модели систем мониторинга АСЗИ				
5. Определение структуры систем мониторинга информационной безопасности	0	4	5, 7	Структура систем мониторинга информационной безопасности
Дидактическая единица: Методы и модели оценки эффективности систем мониторинга				
6. Задачи планирования функционирования систем мониторинга информационной безопасности	0	4	5, 7	Планирования функционирования систем мониторинга информационной безопасности
7. Оптимальное построение систем мониторинга информационной безопасности.	0	4	6, 7	Оптимальное построение систем мониторинга информационной безопасности.

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 8				
1	РГЗ	2, 5, 6	37	10
: 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. - Москва, 2009. - 330, [1] с. : ил., табл.				
2	Подготовка к занятиям	1, 2, 3	20	5

: Ищейнов В. Я. Защита конфиденциальной информации : [учебное пособие для вузов по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации"] / В. Я. Ищейнов, М. В. Мецатунян. - М., 2009. - 254 с. : ил., табл.				
3	Дополнительная учебная деятельность	1, 3	49	0
: Ищейнов В. Я. Защита конфиденциальной информации : [учебное пособие для вузов по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации"] / В. Я. Ищейнов, М. В. Мецатунян. - М., 2009. - 254 с. : ил., табл. 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. - Москва, 2009. - 330, [1] с. : ил., табл.				
4	Подготовка к аттестации	1, 3	19	2
: Ищейнов В. Я. Защита конфиденциальной информации : [учебное пособие для вузов по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации"] / В. Я. Ищейнов, М. В. Мецатунян. - М., 2009. - 254 с. : ил., табл. 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. - Москва, 2009. - 330, [1] с. : ил., табл.				

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
Контроль	Портал НГТУ
Размещение учебных материалов	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	Мин. балл	Максимальный балл
Семестр: 8		
Подготовка к занятиям:	0	
Практические занятия:	0	
РГЗ: Методы и модели оценки эффективности систем мониторинга	30	60
Контролирующие материалы приводятся в "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. - Москва, 2009. - 330, [1] с. : ил., табл."		
Экзамен:	0	40
Контролирующие материалы (список вопросов) приводятся в "Ищейнов В. Я. Защита конфиденциальной информации : [учебное пособие для вузов по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации"] / В. Я. Ищейнов, М. В. Мецатунян. - М., 2009. - 254 с. : ил., табл."		

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.17	з1. знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем		+
	у2. уметь проводить инструментальный мониторинг защищенности автоматизированных систем	+	+
ПК.24	у1. уметь выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем		+
ПК.27	з1. знать методы и средства проведения аудита и мониторинга безопасности информационных систем	+	+
ПСК.35	у2. уметь внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах	+	+

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

7. Литература

Основная литература

1. 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.

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. Ищейнов В. Я. Защита конфиденциальной информации : [учебное пособие для вузов по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации"] / В. Я. Ищейнов, М. В. Мецатунян. - М., 2009. - 254 с. : ил., табл.

2. 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. - Москва, 2009. - 330, [1] с. : ил., табл.

8.2 Специализированное программное обеспечение

1 Windows

2 Office

9. Материально-техническое обеспечение

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Компьютеры объединены в локальную сеть с выходом в Internet

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

Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Новосибирск 2017

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

Обобщенная структура фонда оценочных средств по **дисциплине** Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей 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.17/КА способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	з1. знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	Дестабилизирующие воздействия на защищённые компьютерные сети и их нейтрализация. Задачи, решаемые при проведении анализа скрытых каналов и порядок проведения анализа скрытых каналов для продуктов и систем ИТ и АС Определение условий функционирования систем мониторинга информационной безопасности АСЗИ Принципы организации и этапы разработки систем мониторинга информационной безопасности АСЗИ. Разработка модели систем мониторинга информационной безопасности АСЗИ. Цели и задачи управление безопасностью информационной инфраструктурой.		Экзамен, вопросы...
ПК.17/КА	у2. уметь проводить инструментальный мониторинг защищенности автоматизированных систем	Дестабилизирующие воздействия на защищённые компьютерные сети и их нейтрализация. Задачи, решаемые при проведении анализа скрытых каналов и порядок проведения анализа скрытых каналов для продуктов и систем ИТ и АС Методы и модели оценки эффективности систем мониторинга информационной безопасности АСЗИ. Определение возможностей несанкционированного доступа к защищаемой информации Принципы организации и этапы разработки систем мониторинга информационной безопасности АСЗИ. Разработка модели систем мониторинга	РГЗ, разделы...	Экзамен, вопросы...

		информационной безопасности АСЗИ.		
ПК.24/Э способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	у1. уметь выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем	Дестабилизирующие воздействия на защищённые компьютерные сети и их нейтрализация. Задачи, решаемые при проведении анализа скрытых каналов и порядок проведения анализа скрытых каналов для продуктов и систем ИТ и АС Методы и модели оценки эффективности систем мониторинга информационной безопасности АСЗИ. Определение возможностей несанкционированного доступа к защищаемой информации Определение компонентов систем мониторинга информационной безопасности АСЗИ Принципы и методы планирования функционирования систем мониторинга информационной безопасности АСЗИ Состав и содержание контроля функционирования систем мониторинга информационной безопасности АСЗИ. Технологическое и организационное обеспечение построения систем мониторинга информационной безопасности АСЗИ.		Экзамен, вопросы...
ПК.27/Э способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	з1. знать методы и средства проведения аудита и мониторинга безопасности информационных систем	Задачи, решаемые при проведении анализа скрытых каналов и порядок проведения анализа скрытых каналов для продуктов и систем ИТ и АС Определение компонентов систем мониторинга информационной безопасности АСЗИ Определение условий функционирования систем мониторинга информационной безопасности АСЗИ Принципы и методы планирования функционирования систем мониторинга информационной безопасности АСЗИ Состав и содержание контроля функционирования систем мониторинга	РГЗ, разделы...	Экзамен, вопросы...

		информационной безопасности АСЗИ. Технологическое и организационное обеспечение построения систем мониторинга информационной безопасности АСЗИ.		
ПСК.35 способность проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов	у2. уметь внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах	Задачи планирования функционирования систем мониторинга информационной безопасности Методика выявления состава систем мониторинга информационной безопасности Методы решения задач мониторинга информационной безопасности Определение структуры систем мониторинга информационной безопасности Оптимальное построение систем мониторинга информационной безопасности. Разработка политики безопасности и регламента мониторинга Система управления информационной безопасностью предприятия.	РГЗ, разделы...	Экзамен, вопросы...

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 8 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ПК.17/КА, ПК.24/Э, ПК.27/Э, ПСК.35.

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

В 8 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.17/КА, ПК.24/Э, ПК.27/Э, ПСК.35, 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 «Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей», 8 семестр

1. Методика оценки

Экзамен проводится в устной (письменной) форме, по билетам (тестам). Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов ____, второй вопрос из диапазона вопросов ____ (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 «Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей»

---

1. Вопрос 1
2. Вопрос 2.

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 *45 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, например, вычислительные, оценка составляет *65 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 *85 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 100 *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 «Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей»

1. Процессы жизненного цикла систем ГОСТ Р ИСО/МЭК 15288—2005.
2. Процессы жизненного цикла программных средств ГОСТ Р ИСО/МЭК 12207.
3. Порядок создания АСЗИ. Общие положения ГОСТ Р 51583-2014.
4. Стадии и этапы работ по созданию АСЗИ - ГОСТ 34.601.
5. Содержание работ в части создания системы ЗИ.
6. Содержание и порядок выполнения работ по ЗИ о создаваемой АСЗИ.
7. Требования по разработке документации на АСЗИ.
8. Требования к управлению проектом ГОСТ Р 54869.
9. Виды испытаний АСЗИ и общие требования к их проведению.
10. Испытания АСЗИ на соответствие требованиям безопасности информации.
11. Аттестация АСЗИ для подтверждения соответствия системы ЗИ АСЗИ.
12. Формирование требований к системе ЗИ АСЗИ с учетом ГОСТ Р ИСО/МЭК 27005.
13. Формирование требований к системе ЗИ АСЗИ с учетом ГОСТ Р ИСО/МЭК 21827.
14. Формирование требований к системе ЗИ АСЗИ с учетом ГОСТ Р ИСО/МЭК27002.
15. Разработка концепции АС с учетом ГОСТ Р ИСО/МЭК ТО 19791.
16. Разработка концепции АС с учетом ГОСТ Р ИСО/МЭК 21827.
17. Разработка концепции АС с учетом ГОСТ Р ИСО/МЭК27002.

18. Разработка концепции АС с учетом ГОСТР ИСО/МЭК ТО 15446
19. Состав работ на стадии «Техническое задание» в соответствии с требованиями ГОСТ 34.602.
20. Состав работ на стадии «Техническое задание» с учетом ГОСТ Р ИСО/МЭК ТО 19791.
21. Состав работ на стадии «Техническое задание» с учетом ГОСТР ИСО/МЭК ТО 15446.
22. Состав работ на стадии «Техническое задание» с учетом ГОСТР ИСО/МЭК 15408-1,2.
23. Разработка (проектирование) системы ЗИ на стадиях создания АСЗИ в соответствии с требованиями ГОСТ 34.601.
24. Работы выполняемые при создании системы ЗИ создаваемой (модернизируемой) АСЗИ на стадии "Эскизный проект".
25. Этап "Разработка предварительных проектных решений по системе и ее частям". Определение функций системы ЗИ создаваемой (модернизируемой) АСЗИ, состава комплексов задач и отдельных задач, решаемых подсистемой ЗИ.
26. Этап "Разработка предварительных проектных решений по системе и ее частям". Определение функций и параметров ТС и ПС системы ЗИ.
27. Работы выполняемые при создании системы ЗИ создаваемой (модернизируемой) АСЗИ на этапе "Разработка документации на АС и ее части" стадии "Эскизный проект". Виды документов - по ГОСТ 34.201.
28. Состав работ стадии "Технический проект". Виды документов.
29. Состав работ на стадии "Рабочая документация" в соответствии с требованиями РД 50-34.698-90.
30. Работы выполняемые при создании системы ЗИ создаваемой (модернизируемой) АСЗИ на этапе "Разработка документации на АС и ее части" стадии "Рабочая документация" с учетом ГОСТР ИСО/МЭК 15408-1,3.
31. Состав работ на стадии "Рабочая документация" этапе "Разработка и адаптация программ".
32. Внедрение системы ЗИ АСЗИ.
33. Аттестация АСЗИ на соответствие требованиям безопасности информации.
34. Сопровождение системы ЗИ в ходе эксплуатации АСЗИ.
35. Состав работ стадии " Ввод в действие " с учетом ГОСТР ИСО/МЭК 15408-1,3.
36. Состав работ стадии " Ввод в действие " с учетом ГОСТР ИСО/МЭК 18045.
37. Содержание и порядок выполнения работ по защите информации о создаваемой АСЗИ.

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

Паспорт
расчетно-графического задания (работы)

по дисциплине «Современные методы и средства мониторинга информационной безопасности и защиты компьютерных сетей», 8 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны рассчитать параметры элементов системы мониторинга и управления индентами

При выполнении расчетно-графического задания (работы) студенты должны провести анализ объекта диагностирования, выбрать и обосновать диагностические признаки и параметры, разработать алгоритмы диагностирования, выбрать аппаратные средства.

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), отсутствует анализ объекта, диагностические признаки не обоснованы, аппаратные средства не выбраны или не соответствуют современным требованиям, оценка составляет 45 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы, аппаратные средства не соответствуют современным требованиям, оценка составляет 65 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 средства выбраны без достаточного обоснования, оценка составляет 85 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 средств обоснован, оценка составляет 100 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. Принцип работы систем мониторинга и управления индентами в компьютерных сетях.
2. Принцип работы систем анализа защищенности компьютерных сетей.
3. Принцип работы систем контроля привилегированных пользователей.
4. Принцип работы систем контроля конфиденциальной информации в компьютерных сетях.
5. Принцип работы систем борьбы с целенаправленными атаками в информационных системах.
6. Принцип работы систем защиты от бот и DDos атак.