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
Дополнительные главы защиты информации на критически важных объектах

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)	5
2	Всего часов	180
3	Всего занятий в контактной форме, час.	68
4	Лекции, час.	18
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.	12
10	Самостоятельная работа, час.	112
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*: ПСК.32 способность участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов; *в части следующих результатов обучения*:**
з1. знать средства защиты информации, используемые на критически важных объектах
***Компетенция ФГОС*: ПСК.34 способность разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов; *в части следующих результатов обучения*:**
у1. уметь формировать политики безопасности для критически важных объектов
у2. уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью критически важных объектов
***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*:**
з1. знать терминологию и системный подход к построению защищенных автоматизированных систем критически важных объектов
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
Дополнительные главы защиты информации на критически важных объектах	
ПСК.32.з1 знать средства защиты информации, используемые на критически важных объектах	
1.Формальные модели безопасности компьютерных систем и сетей	Лекции; Самостоятельная работа
ПСК.34.у1 уметь формировать политики безопасности для критически важных объектов	
2.Анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия	Лекции; Практические занятия; Самостоятельная работа
ПСК.34.у2 уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью критически важных объектов	
3.Применять методы анализа защищенности компьютерных систем и сетей	Лекции; Практические занятия; Самостоятельная работа
ПСК.35.з1 знать терминологию и системный подход к построению защищенных автоматизированных систем критически важных объектов	
4.Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Лекции; Самостоятельная работа
ПСК.35.у2 уметь внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах	
5.Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику	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: Обеспечение безопасности информационной инфраструктуры предприятия				
1. Цели и задачи обеспечения безопасности и углубленного анализа информационной инфраструктуры предприятия	0	2	1, 4	
2. Принципы и методы обеспечения безопасности и углубленного анализа информационной инфраструктуры предприятия	0	2	4	Методы обеспечения безопасности и углубленного анализа информационной инфраструктуры предприятия
3. Моделирование безопасности и углубленного анализа информационной инфраструктуры предприятия	0	4	1, 4	Модели безопасности и углубленного анализа информационной инфраструктуры предприятия
Дидактическая единица: Проектирование безопасности и углубленного анализа информационной инфраструктуры предприятия				
4. Руководящие и методические документы регламентирующие разработку ситемы безопасности инфраструктуры предприятия	0	4	4	Методы разработки ситемы безопасности инфраструктуры предприятия
Дидактическая единица: Оценки эффективности систем безопасности информационной инфраструктуры предприятия				
5. Принципы и методы оценки безопасности и углубленного анализа информационной инфраструктуры предприятия	2	4	1, 2	Способы оценки безопасности и углубленного анализа информационной инфраструктуры предприятия
6. Международная практика обеспечения безопасности информационной инфраструктуры предприятия	2	2	1, 3	Международная практика обеспечения безопасности

Таблица 3.2

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 8				
Дидактическая единица: Обеспечение безопасности информационной инфраструктуры предприятия				
1. Средства обеспечения безопасности и углубленного анализа NETCAT и CRYPTCAT	2	4	2	NETCAT и CRYPTCAT средства обеспечения безопасности и углубленного анализа сети.
Дидактическая единица: Проектирование безопасности и углубленного анализа информационной инфраструктуры предприятия				
2. Комбинированные средства системного аудита	2	6	3, 5	Современные средства системного аудита
3. Использование набора инструментов для расследования атак в системе Windows	2	4	2	Компоновка набора инструментов для расследования атак в системе Windows
4. Использование комплекта инструментов расследования атак для Unix	2	4	5	Применение комплекта инструментов расследования атак для Unix
Дидактическая единица: Оценки эффективности систем безопасности информационной инфраструктуры предприятия				

5. Применение средств судебного дублирования	2	6	2, 5	Средства судебного дублирования
6. Использование средств судебного анализа.	2	6	2, 5	Способы судебного анализа.
7. Инструментальные средства для реконструкции деятельности нарушителя	2	6	2, 3, 5	Способы реконструкции деятельности нарушителя

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 8				
1	РГЗ	2, 3	48	4
: Воробьев Л. В. Системы и сети передачи информации : [учебное пособие для вузов по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем"] / Л. В. Воробьев, А. В. Давыдов, Л. П. Щербина. - М., 2009. - 328, [1] с. : схемы Проскурин В. Г. Защита программ и данных : [учебное пособие для вузов по специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем"] / В. Г. Проскурин. - М., 2011. - 198, [1] с.				
2	Подготовка к занятиям	1, 2, 3, 4	28	6
: Варлатая С. К. Защита информационных процессов в компьютерных сетях : учебно-методический комплекс / С. К. Варлатая, М. В. Шаханова. - Москва, 2017 Воробьев Л. В. Системы и сети передачи информации : [учебное пособие для вузов по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем"] / Л. В. Воробьев, А. В. Давыдов, Л. П. Щербина. - М., 2009. - 328, [1] с. : схемы Проскурин В. Г. Защита программ и данных : [учебное пособие для вузов по специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем"] / В. Г. Проскурин. - М., 2011. - 198, [1] с.				
3	Подготовка к аттестации	1, 4	36	2
: Бабаш А. В. Информационная безопасность. Лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - М., 2012. - 131 с. : табл., ил. + 1 CD-ROM. 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. Воробьев Л. В. Системы и сети передачи информации : [учебное пособие для вузов по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем"] / Л. В. Воробьев, А. В. Давыдов, Л. П. Щербина. - М., 2009. - 328, [1] с. : схемы				

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	Портал НГТУ
Консультирование	Портал НГТУ; Среда электронного обучения НГТУ
Контроль	Среда электронного обучения НГТУ
Размещение учебных материалов	Среда электронного обучения НГТУ

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		
Практические занятия:	10	20
Контролирующие материалы приводятся в "Воробьев Л. В. Системы и сети передачи информации : [учебное пособие для вузов по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем"] / Л. В. Воробьев, А. В. Давыдов, Л. П. Щербина. - М., 2009. - 328, [1] с. : схемы"		
РГЗ:	20	40
Контролирующие материалы приводятся в "Варлатая С. К. Защита информационных процессов в компьютерных сетях : учебно-методический комплекс / С. К. Варлатая, М. В. Шаханова. - Москва, 2017"		
Экзамен:	20	40
Контролирующие материалы (список вопросов) приводятся в "Проскурин В. Г. Защита программ и данных : [учебное пособие для вузов по специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем"] / В. Г. Проскурин. - М., 2011. - 198, [1] с."		

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
ПСК.32	з1. знать средства защиты информации, используемые на критически важных объектах		+
ПСК.34	у1. уметь формировать политики безопасности для критически важных объектов	+	
	у2. уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью критически важных объектов	+	
ПСК.35	з1. знать терминологию и системный подход к построению защищенных автоматизированных систем критически важных объектов		+
	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. Грушо А. А. Теоретические основы компьютерной безопасности : [учебное пособие по специальностям 090100 "Информационная безопасность"] / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М., 2009. - 267, [1] с. : ил.

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.

3. Девянин П. Н. Модели безопасности компьютерных систем : учебное пособие для вузов по специальностям 075200 "Компьютерная безопасность" и 075500 "Комплексное обеспечение информационной безопасности автоматизированных систем" / П. Н. Девянин. - М., 2005. - 142, [1] 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. Проскурин В. Г. Защита программ и данных : [учебное пособие для вузов по специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем"] / В. Г. Проскурин. - М., 2011. - 198, [1] с.

2. Бабаш А. В. Информационная безопасность. Лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - М., 2012. - 131 с. : табл., ил. + 1 CD-ROM.

3. Воробьев Л. В. Системы и сети передачи информации : [учебное пособие для вузов по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем"] / Л. В. Воробьев, А. В. Давыдов, Л. П. Щербина. - М., 2009. - 328, [1] с. : схемы

4. 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.

5. Варлатая С. К. Защита информационных процессов в компьютерных сетях : учебно-методический комплекс / С. К. Варлатая, М. В. Шаханова. - Москва, 2017

8.2 Специализированное программное обеспечение

1 Подписка Imagine Premium

9. Материально-техническое обеспечение

Компьютерный класс

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

Лабораторный стенд

№	Наименование	Назначение
1	Компьютерный класс№4	проведение занятий
2	Компьютерный комплекс контроля доспупа в составе	проведение занятий

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

Дополнительные главы защиты информации на критически важных объектах
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** Дополнительные главы защиты информации на критически важных объектах 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)**
ПСК.32 способность участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	з1. знать средства защиты информации, используемые на критически важных объектах	Международная практика обеспечения безопасности информационной инфраструктуры предприятия Моделирование безопасности и углубленного анализа информационной инфраструктуры предприятия Принципы и методы оценки безопасности и углубленного анализа информационной инфраструктуры предприятия Цели и задачи обеспечения безопасности и углубленного анализа информационной инфраструктуры предприятия		Экзамен, вопросы...
ПСК.34 способность разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	у1. уметь формировать политики безопасности для критически важных объектов	Инструментальные средства для реконструкции деятельности нарушителя Использование средств судебного анализа. Применение средств судебного дублирования Средства обеспечения безопасности и углубленного анализа NETCAT и CRYPTCAT	РГЗ, разделы...	
ПСК.34	у2. уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью критически важных объектов	Инструментальные средства для реконструкции деятельности нарушителя Комбинированные средства системного аудита Международная практика обеспечения безопасности информационной инфраструктуры предприятия	РГЗ, разделы...	
ПСК.35 способность проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически	з1. знать терминологию и системный подход к построению защищенных автоматизированных систем критически важных объектов	Моделирование безопасности и углубленного анализа информационной инфраструктуры предприятия Принципы и методы обеспечения безопасности и углубленного анализа информационной инфраструктуры предприятия Руководящие и методические документы		Экзамен, вопросы...

важных объектах и в автоматизированных системах критически важных объектов		регламентирующие разработку ситемы безопасности инфраструктуры предприятия Цели и задачи обеспечения безопасности и углубленного анализа информационной инфраструктуры предприятия		
ПСК.35	у2. уметь внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах	Использование средств судебного анализа. Применение средств судебного дублирования		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 ПСК.32, ПСК.34, 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 ПСК.32, ПСК.34, 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 «Дополнительные главы защиты информации на критически важных объектах», 8 семестр

1. **Методика оценки**

1. **Методика оценки**

Экзамен проводится в устной (письменной) форме, по билетам (тестам). Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-18, второй вопрос из диапазона вопросов 19-34 (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 «Дополнительные главы защиты информации на критически важных объектах»

1. Цели, задачи и принципы построения систем обеспечения информационной безопасности защищённых компьютерных сетей.
2. Понятия безопасности и защищенности, достаточность систем мониторинга информационной безопасности защищённых компьютерных сетей.
3. Стандарты управления безопасностью предприятия и обеспечение информационной безопасности защищённых компьютерных сетей.
4. Цели и задачи систем мониторинга информационной безопасности защищённых компьютерных сетей.
5. Методологические основы организации и этапы разработки систем обеспечения информационной безопасности защищённых компьютерных сетей.
6. Разработка политики безопасности и регламента безопасности предприятия. Системы обеспечения информационной безопасности защищённых компьютерных сетей

7. Формализация целей функционирования и формирование системы критериев оптимальности систем обеспечения информационной безопасности защищённых компьютерных сетей.
8. Система управления информационной безопасностью предприятия. Функции систем обеспечения информационной безопасности защищённых компьютерных сетей.
9. Требования, предъявляемые к организационной, технической составляющим систем обеспечения информационной безопасности защищённых компьютерных сетей.
10. Факторы, определяющие построение и организацию систем обеспечения информационной безопасности защищённых компьютерных сетей.
11. Определение объектов защиты. Методика выявления носителей защищаемой информации.
12. Определение объектов защиты. Особенности взаимоотношений с контрагентами.
13. Обеспечение безопасности информации в непредвиденных ситуациях.
14. Реагирование на инциденты ИБ.
15. Резервирование информации и отказоустойчивость
16. Безопасность «облачных» вычислений.
17. Задачи защищённых по выявлению угроз и мониторингу информационной безопасности защищённых компьютерных сетей.
18. Классификация СЗИ компьютерных сетей и методы обеспечения безопасности информации.
19. Определение компонентов систем обеспечения информационной безопасности защищённых компьютерных сетей. Синтез СЗИ компьютерных сетей от НСД.
20. Оптимальное построение системы защиты и определение структуры СЗИ компьютерных сетей. Особенности проектирования системы защиты информации для существующих компьютерных сетей.
21. Определение условий функционирования систем обеспечения информационной безопасности компьютерных сетей. Разделы концепции построения систем мониторинга информационной безопасности компьютерных сетей их содержание.
22. Общая характеристика задач моделирования систем обеспечения информационной безопасности компьютерных сетей. Формальные и прикладные модели безопасности и их анализ.
23. Разработка модели систем обеспечения информационной безопасности компьютерных сетей. Формализация модели безопасности.

24. Общее содержание работ по организации систем обеспечения информационной безопасности компьютерных сетей и характеристика основных стадий создания .
25. Назначение и структура технического задания, предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию.
26. Понятие, сущность, цели и принципы систем управления информационной безопасностью защищённых компьютерных сетей.
27. Структура, процессы, функции и задачи управления информационной безопасностью защищённых компьютерных сетей. Структура и содержание общей технологии управления.
28. Принципы и методы планирования функционирования систем мониторинга информационной безопасности компьютерных сетей.
29. Сущность и содержание контроля функционирования систем информационной безопасности компьютерных сетей.
30. Функционирование системы управления информационной безопасностью. Аудит и мониторинг безопасности.
31. Управление системой информационной безопасности компьютерных сетей в условиях чрезвычайных ситуаций.
32. Характеристика подходов к оценке эффективности систем информационной безопасности компьютерных сетей. Вероятностный и оценочный подходы.
33. Методы и модели оценки эффективности систем информационной безопасности компьютерных сетей. Показатель уровня защищенности, основанный на экспертных оценках
34. Методы и модели оценки эффективности систем информационной безопасности компьютерных сетей. Методы проведения экспертного опроса
35. Методы и модели оценки эффективности систем информационной безопасности компьютерных сетей. Экономический подход к оценке эффективности защищённых АС.

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

Паспорт
расчетно-графического задания (работы)

по дисциплине «Дополнительные главы защиты информации на критически важных объектах», 8 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны рассчитать параметры элементов системы безопасности автоматизированных систем (АС) критически важных объектов (КВО) в условиях существования угроз в информационной сфере.

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

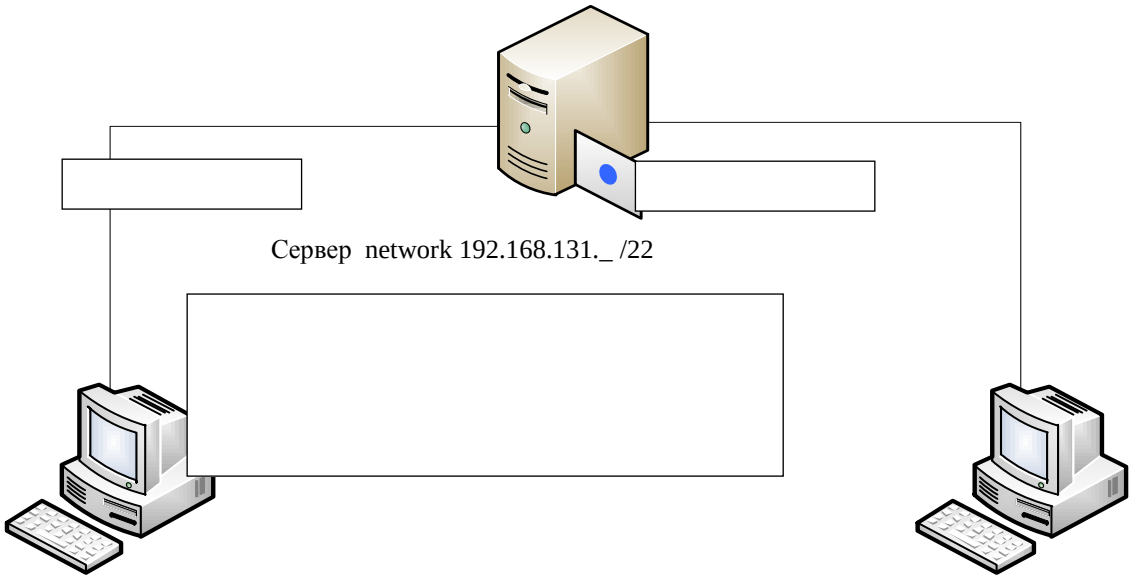
В общей оценке по дисциплине баллы за РГЗ(Р) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Примерный перечень тем РГЗ(Р)

- Для заданного рис. сегмента корпоративной сети применить :
- Инструментальные средства проверки TCP/IP-стека.
- Компоновка и использование набора инструментов для расследования хакерских атак, то есть для "живого ответа" в системе Windows.
- Создание и использование комплекта инструментов "живого ответа" для Unix.
- Коммерческие наборы инструментов для судебного дублирования.
- Некоммерческие наборы инструментов, предназначенные для судебного

дублирования.

- Наборы инструментов , помогающие при судебном анализе.
- Инструментальные средства, помогающие реконструировать деятельность , связанную с интернетом.



5.

6. VM1 Debian VM2 Windows 7

networks: 192.168.132._/29 network 192.168.133._/29

8.

9. Рис. Конфигурация тестовой подсети

10.

11.