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
Специальные вопросы защиты информации

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

Курс: 5, семестр : 9

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**9**
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.	8
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:

профессор, д.т.н. Абденов А. Ж.

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*: ОПК.2 способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники; *в части следующих результатов обучения*:**
з2. знать базовые положения фундаментальных разделов математики в объеме, необходимом для владения математическим аппаратом для обработки информации и анализа данных в области профессиональной деятельности
з3. знать природу возникновения погрешностей при применении математических моделей и необходимости оценивать погрешность
з4. знать универсальность математических методов в познании окружающего мира
у5. уметь применять основные методы математического аппарата в математических моделях объектов и процессов

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	Формы организации занятий
Специальные вопросы защиты информации	
ОПК.2.з2 знать базовые положения фундаментальных разделов математики в объеме, необходимом для владения математическим аппаратом для обработки информации и анализа данных в области профессиональной деятельности	
1.основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	Лекции; Практические занятия; Самостоятельная работа
ОПК.2.з3 знать природу возникновения погрешностей при применении математических моделей и необходимости оценивать погрешность	
2.возможности технических средств перехвата информации;	Лекции; Практические занятия; Самостоятельная работа
ОПК.2.у5 уметь применять основные методы математического аппарата в математических моделях объектов и процессов	
3.методами расчета и инструментального контроля показателей технической защиты информации;	Лекции; Практические занятия; Самостоятельная работа
4.методами формирования требований по защите информации;	Лекции; Практические занятия; Самостоятельная работа
5.методами и средствами технической защиты информации;	Лекции; Практические занятия; Самостоятельная работа
ОПК.2.з4 знать универсальность математических методов в познании окружающего мира	
6.автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;	Лекции; Практические занятия; Самостоятельная работа
ОПК.2.у5 уметь применять основные методы математического аппарата в математических моделях объектов и процессов	
7.методами организации и управления деятельностью служб защиты информации на предприятии;	Лекции; Практические занятия
8.определять комплекс мер правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;	Лекции; Практические занятия
9.выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем;	Лекции; Практические занятия

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 9			
Дидактическая единица: Система управления информационной безопасностью			
1. Информационная безопасность как обеспечение непрерывности бизнеса	0	6	1, 2, 3
Дидактическая единица: Эффективность бизнес-процессов			
2. Анализ информационных рисков	0	6	2, 3, 4
Дидактическая единица: Количественная оценка рисков; Качественная оценка рисков; Типы, виды, область распространения политик безопасности			
3. Политики информационной безопасности, оценка рисков.	0	8	4, 5, 7
Дидактическая единица: Методы, способы проведения аудита			
4. Аудит информационной безопасности.	0	8	6, 8, 9
Дидактическая единица: Мониторинг, планирование, восстановление информационных систем			
5. Реагирование на инциденты информационной безопасности	0	8	8, 9

Таблица 3.2

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 9				
Дидактическая единица: Система управления информационной безопасностью				
1. NIST Special Publication 800-60, Information Security. Guide for Mapping Types of Information and Information Systems to Security Categories. Разработка и документирование методики категорирования информационных ресурсов в зависимости от возможных потерь для бизнеса вследствие нарушений целостности и/или доступности и/или конфиденциальности информации, информационных систем.	0	4	1, 2, 3	студенты осваивают методы категорирования активов по индивидуальным заданиям. Теоретическими фактами защищают и обосновывают

5. Организационная роль информационной безопасности	0	4	3, 4, 8	Организационная роль информационной безопасности на основании ГОСТ ИСО/МЭК 15408-2202. Практическая архитектура живучести систем и сетей Петера Ньюмена. Международный стандарт ISO/IEC 17799:2005 Information technology-Security techniques-Code of practice for information security management. Система управления информационной безопасностью как часть общей системы менеджмента. Административное взаимодействие CISO, BISO. Сравнение основных положений законодательной базы РФ и зарубежных, международных стандартов. Категорирование ресурсов с точки зрения рисков потери целостности, доступности, конфиденциальности. Адаптивная модель управления безопасностью Internet Security Systems
Дидактическая единица: Эффективность бизнес-процессов				
2. NIST Special Publication 800-53. Recommended Security Controls for Federal Information Systems. Разработка и документирование организационно-технических требований обеспечения безопасности информационных ресурсов (отдельные разделы).	0	4	1, 3, 4	Студенты занимаются разработкой и документированием организационно-технических требований обеспечения безопасности информационных ресурсов
3. ISO/IEC 17799:2005 Information technology-Security techniques-Code of practice for information security management. Разработка и документирование отдельных подсистем системы менеджмента информационной безопасности.	0	4	6, 7, 8	Студенты занимаются разработкой и документированием отдельных подсистем системы менеджмента информационной безопасности.
Дидактическая единица: Количественная оценка рисков; Качественная оценка рисков; Типы, виды, область распространения политик безопасности				

6. Методы оценки рисков, способы управления рисками	2	4	1, 4	Сравнение зарубежных стандартов в части ориентированности на управление рисками. Методы оценки рисков, способы управления рисками. Руководство по управлению рисками в ИТ-системах NIST SP 800-30. Стадии по управлению информационными рисками согласно NIST SP 800-30. Количественная оценка рисков. Качественная оценка рисков. Инструментальные средства оценки и управления информационными рисками. Особые угрозы информационной безопасности (социальный инжиниринг, инсайдеры). Способы манипулирования людьми. Пирамида мотиваций.
7. Политика безопасности	0	4	6, 8, 9	Принципы разделения полномочий и минимизации привилегий. Иерархическая модель политик безопасности. Типы, виды, область распространения политик безопасности. Правила разработки и документирования политик безопасности согласно требованиям международных стандартов. Стадии развития, правила успешности ASP. Континуум обучения информационной безопасности в организации согласно NIST SP 800-16. Способы продвижения политик безопасности.
Дидактическая единица: Методы, способы проведения аудита				
4. ISO/IEC 27001:2005 Information technology-Security techniques-Information security management systems-Requirements. Разработка и документирование методики аудита информационной безопасности по отдельным группам контролей.	4	4	5, 6, 7	Занимаются разработкой и документированием методики аудита информационной безопасности по отдельным группам контролей.
Дидактическая единица: Мониторинг, планирование, восстановление информационных систем				

8. Мониторинг	2	8	5, 6, 8	Мониторинг. Ситуационные центры. Планирование восстановления функционирования информационных систем в случаях нештатных ситуаций. Recovery point object. Recovery time object.

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 9				
1	РГЗ	3, 4, 5	30	0
: Бузов Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г. А. Бузов. - М., 2010. - 237 с. : ил.				
2	Подготовка к занятиям	1, 2, 6	23	0
: Бузов Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г. А. Бузов. - М., 2010. - 237 с. : ил.				
3	Дополнительная учебная деятельность	1, 2	32	15
: Бузов Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г. А. Бузов. - М., 2010. - 237 с. : ил.				
4	Подготовка к аттестации	2, 3, 6	40	2
: Бузов Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г. А. Бузов. - М., 2010. - 237 с. : ил.				

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; Социальные сети

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: 9	
Лекция:	20

Практические занятия:	60
РГЗ:	
Экзамен:	40
Контролирующие материалы - список вопросов	

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
ОПК.2	з2. знать базовые положения фундаментальных разделов математики в объеме, необходимом для владения математическим аппаратом для обработки информации и анализа данных в области профессиональной деятельности		+
	з3. знать природу возникновения погрешностей при применении математических моделей и необходимости оценивать погрешность		+
	з4. знать универсальность математических методов в познании окружающего мира	+	+
	у5. уметь применять основные методы математического аппарата в математических моделях объектов и процессов	+	+

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

7. Литература

Основная литература

1. Конеев И. Р. Информационная безопасность предприятия / Искандер Конеев, Андрей Беляев. - СПб., 2003. - 733 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. Бузов Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г. А. Бузов. - М., 2010. - 237 с. : ил.

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)	Презентационные материалы

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

Специальные вопросы защиты информации

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** Специальные вопросы защиты информации 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)**
ОПК.2 способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	з1. знать базовые положения фундаментальных разделов математики в объеме, необходимом для владения математическим аппаратом для обработки информации и анализа данных в области профессиональной деятельности	NIST Special Publication 800-53. Recommended Security Controls for Federal Information Systems. Разработка и документирование организационно-технических требований обеспечения безопасности информационных ресурсов (отдельные разделы). NIST Special Publication 800-60, Information Security. Guide for Mapping Types of Information and Information Systems to Security Categories. Разработка и документирование методики категорирования информационных ресурсов в зависимости от возможных потерь для бизнеса вследствие нарушений целостности и/или доступности и/или конфиденциальности информации, информационных систем. Информационная безопасность как обеспечение непрерывности бизнеса Методы оценки рисков, способы управления рисками		Экзамен, вопросы...
ОПК.2	з2. знать природу возникновения погрешностей при применении математических моделей и необходимости оценивать погрешность	NIST Special Publication 800-60, Information Security. Guide for Mapping Types of Information and Information Systems to Security Categories. Разработка и документирование методики категорирования информационных ресурсов в зависимости от возможных потерь для бизнеса вследствие нарушений целостности и/или доступности и/или конфиденциальности информации, информационных систем. Анализ информационных рисков Информационная безопасность как обеспечение непрерывности бизнеса		Экзамен, вопросы...

ОПК.2	з3. знать универсальность математических методов в познании окружающего мира	ISO/IEC 17799:2005 Information technology-Security techniques-Code of practice for information security management. Разработка и документирование отдельных подсистем системы менеджмента информационной безопасности. ISO/IEC 27001:2005 Information technology-Security techniques-Information security management systems-Requirements. Разработка и документирование методики аудита информационной безопасности по отдельным группам контролей. Аудит информационной безопасности. Мониторинг Политика безопасности	РГЗ, разделы...	Экзамен, вопросы...
ОПК.2	у3. уметь применять основные методы математического аппарата в математических моделях объектов и процессов	ISO/IEC 17799:2005 Information technology-Security techniques-Code of practice for information security management. Разработка и документирование отдельных подсистем системы менеджмента информационной безопасности. ISO/IEC 27001:2005 Information technology-Security techniques-Information security management systems-Requirements. Разработка и документирование методики аудита информационной безопасности по отдельным группам контролей. NIST Special Publication 800-53. Recommended Security Controls for Federal Information Systems. Разработка и документирование организационно-технических требований обеспечения безопасности информационных ресурсов (отдельные разделы). NIST Special Publication 800-60, Information Security. Guide for Mapping Types of Information and Information Systems to Security Categories. Разработка и документирование методики категорирования информационных ресурсов в зависимости от возможных потерь для бизнеса вследствие нарушений целостности и/или доступности и/или конфиденциальности информации, информационных систем. Анализ информационных рисков Аудит	РГЗ, разделы...	Экзамен, вопросы...

		информационной безопасности. Информационная безопасность как обеспечение непрерывности бизнеса Методы оценки рисков, способы управления рисками Мониторинг Организационная роль информационной безопасности Политика безопасности Политики информационной безопасности, оценка рисков. Реагирование на инциденты информационной безопасности		

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 9 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ОПК.2.

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

В 9 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 компетенции ОПК.2, 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 «Специальные вопросы защиты информации», 9 семестр

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 «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 «Специальные вопросы защиты информации», 9 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)

Методы и средства противодействия террористической деятельности в системах управления критически важных объектов