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

Кафедра автономных информационных и управляющих систем

“УТВЕРЖДАЮ”
ДЕКАН ФЛА
д.т.н. Саленко С. Д.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Методы противодействия техническим разведкам

Образовательная программа: 27.04.04 Управление в технических системах, магистерская программа: Автономные информационные и управляющие системы

Курс: 1, семестр : 2

Факультет летательных аппаратов,

		Семестр
№	**Вид деятельности**	**2**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	61
4	Лекции, час.	36
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	36
8	Аттестация, час.	2
9	Консультации, час.	5
10	Самостоятельная работа, час.	47
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	ДЗ

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 27.04.04 Управление в технических системах

ФГОС введен в действие приказом №1414 от 30.10.2014 г. , дата утверждения: 01.12.2014 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная, по выбору студента

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 27.04.04 Управление в технических системах

Рабочая программа обсуждена на заседании кафедры

АИУС, протокол заседания кафедры №7 от 20.06.2017

Утверждена на совете факультета летательных аппаратов, протокол № 5 от 21.06.2017

Программу разработал:

инженер 2 категории, Литвиненко С. А.

Заведующий кафедрой:

доцент, д.т.н. Легкий В. Н.

Ответственный за образовательную программу:

заведующий кафедрой Легкий В. Н.

1. Внешние требования

Таблица 1.1

***Компетенция НГТУ*: ПК.29.В/ОУ способность соблюдать основные требования информационной безопасности; *в части следующих результатов обучения*:**
з4. знать возможные угрозы информационной безопасности
з5. знать технические мероприятия по защите информации
з6. знать методы защиты информации от утечки по техническим каналам
у2. уметь применять средства автоматического контроля, обнаружения и закрытия возможных каналов утечки защищаемых сведений

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Методы противодействия техническим разведкам	
ПК.29.В/ОУ.з4 знать возможные угрозы информационной безопасности	
1.О видах совершаемых компьютерных преступлений.	Лекции; Самостоятельная работа
2.О возможных угрозах безопасности информации и путях их ликвидации	Лекции; Лабораторные работы; Самостоятельная работа
3.О подборе, приеме, увольнении, расстановке кадров с учетом выявленных особенностей характера и поведения сотрудников в коллективе.	Лекции; Самостоятельная работа
4.Обязанности руководства объекта и персонала при работе с защищаемой информацией	Лекции; Лабораторные работы; Самостоятельная работа
ПК.29.В/ОУ.з5 знать технические мероприятия по защите информации	
5.О состоянии дел в РФ, связанных с правовым регулированием вопросов обеспечения информационной безопасности.	Лекции; Самостоятельная работа
6.О международном законодательстве в области защиты информации.	Лекции; Самостоятельная работа
7.Требования пропускного и внутриобъектового режимов	Лекции; Лабораторные работы; Самостоятельная работа
8.Технологические меры поддержания информационной безопасности объектов	Лекции; Лабораторные работы; Самостоятельная работа
ПК.29.В/ОУ.з6 знать методы защиты информации от утечки по техническим каналам	
9.О видах защищаемой информации (государственная тайна, конфиденциальная информация) и органах её защиты	Лекции; Лабораторные работы; Самостоятельная работа
10.Меры, которыми достигается снижение ущерба от возможной утраты информации;	Лекции; Лабораторные работы; Самостоятельная работа
11.Задачи, решаемые системой инженерной защиты, службой безопасности коммерческого объекта и режимно-секретными органами	Лабораторные работы; Самостоятельная работа
ПК.29.В/ОУ.у2 уметь применять средства автоматического контроля, обнаружения и закрытия возможных каналов утечки защищаемых сведений	
12.Уверенно оценивать правовые аспекты решения задач по защите информации на оборонных и промышленных предприятиях народно-хозяйственного комплекса страны;	Лекции; Самостоятельная работа
13.Анализировать эксплуатационную и иную документацию организаций и подразделений ведомства с целью подготовки решений по совершенствованию подсистем, обеспечивающих защиту информации;	Лекции; Лабораторные работы; Самостоятельная работа
14.Эффективного использовать средства автоматического контроля, обнаружения и закрытия возможных каналов утечки защищаемых сведений;	Лекции; Лабораторные работы; Самостоятельная работа
15.Сертификации ОТСС, ВТСС, средств защиты информации и аттестации объектов информатизации требованиям по безопасности информации.	Лекции; Лабораторные работы; Самостоятельная работа

16.Обеспечения информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного технического и экономического сотрудничества	Лекции; Лабораторные работы; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 2			
Дидактическая единица: Правовое обеспечение коммерческой безопасности			
1. Определение основных понятий	0	4	2, 5, 9
2. Законодательство РФ в области информационной безопасности	0	6	12, 5, 6
3. Понятие и виды защищаемой информации по законодательству РФ	0	4	5, 9
4. Работа с кадрами	0	6	1, 10, 2, 3, 4
Дидактическая единица: Организационно-техническое обеспечение коммерческой безопасности			
5. Организация и обеспечение режима секретности	0	8	12, 13, 14, 16, 7
6. Средства и методы физической защиты объектов	0	8	1, 10, 13, 14, 15, 16, 2, 8

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 2				
Дидактическая единица: Организационно-техническое обеспечение коммерческой безопасности				
1. Составление технического паспорта на выделенное помещение	8	4	10, 13, 16, 7, 8	Получение практических навыков по определению и установлению организационно-технических требований защиты секретной и конфиденциальной речевой информации при её обсуждении в выделенном либо защищаемом помещении (ВП, ЗП).
2. Передача информации по телефонным линиям связи.	8	4	11, 14, 16, 2	Ознакомление с принципами передачи информации по телефонным линиям связи и способами несанкционированного съема информации и способы противодействия им

3. Составление технического паспорта на объект вычислительной техники.	8	4	13, 15, 7, 8	Получение практических навыков по определению и установлению организационно-технических требований защиты секретной и конфиденциальной информации при её обработке в автоматизированной системе (АС).
4. Передача информации по радиоканалу.	4	4	10, 16, 2, 8	Ознакомление с принципами передачи информации по радиоканалу и способами несанкционированного съема информации и способы противодействия им.
5. Составление актов категорирования объекта вычислительной техники и акта классификации автоматизированной системы	8	2	10, 13, 15, 4, 9	Получение практических навыков по категорированию объектов вычислительной техники (ВТ) и выделенных помещений (ВП), предназначенных для обработки (обсуждения) секретной информации, а также классификации автоматизированных систем (АС), предназначенных для обработки секретной и конфиденциальной информации.

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 2				
1	РГЗ	10, 11, 12, 13, 14, 4, 7, 8	10	3
РГЗ студент может построить на "свободных" примерах по темам лекционных и практических занятий, которые позволили бы достаточно объективно оценить уровень подготовки и правильность понимания существа рассматриваемой в данной теме проблемы. Должны быть также представлены определения понятий, используемых в РГЗ.: Соболев А. Н. Физические основы технических средств обеспечения информационной безопасности : [учебное пособие для вузов по специальностям 075500 "Комплексное обеспечение информационной безопасности автоматизированных систем" и 075200 "Компьютерная безопасность"] / А. Н. Соболев, В. М. Кириллов. - М., 2004. - 221, [2] с. : ил.				
2	Подготовка к занятиям	1, 10, 11, 2, 3, 4, 5, 6, 7, 8, 9	22	0
Студентам предлагается повторить предыдущий лекционный, учебно-методический материал. : Соболев А. Н. Физические основы технических средств обеспечения информационной безопасности : [учебное пособие для вузов по специальностям 075500 "Комплексное обеспечение информационной безопасности автоматизированных систем" и 075200 "Компьютерная безопасность"] / А. Н. Соболев, В. М. Кириллов. - М., 2004. - 221, [2] с. : ил.				
3	Дополнительная учебная деятельность	1, 2, 3, 5, 6, 9	5	0
: Соболев А. Н. Физические основы технических средств обеспечения информационной безопасности : [учебное пособие для вузов по специальностям 075500 "Комплексное обеспечение информационной безопасности автоматизированных систем" и 075200 "Компьютерная безопасность"] / А. Н. Соболев, В. М. Кириллов. - М., 2004. - 221, [2] с. : ил.				

4	Подготовка к аттестации	1, 10, 11, 12, 13, 14, 15, 16, 2, 3, 4, 5, 6, 7, 8, 9	10	2
Студентам предлагается ознакомиться с контролирующими материалами, изучить лекционный, учебно-методический материал.: Соболев А. Н. Физические основы технических средств обеспечения информационной безопасности : [учебное пособие для вузов по специальностям 075500 "Комплексное обеспечение информационной безопасности автоматизированных систем" и 075200 "Компьютерная безопасность"] / А. Н. Соболев, В. М. Кириллов. - М., 2004. - 221, [2] 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	Портал НГТУ
Консультирование	e-mail:darron@ngs.ru
Размещение учебных материалов	ЭБС

6. Правила аттестации обучающихся по учебной дисциплине

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

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Мин. балл	Максимальный балл
Семестр: 2		
Лекция:	10	20
Лабораторная:	15	30
РГЗ:	15	30
Зачет:	10	20

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

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля	
		Защита РГЗ	Зачет
	ПК.29.В/ОУ з4. знать возможные угрозы информационной безопасности	+	+
	ПК.29.В/ОУ з5. знать технические мероприятия по защите информации	+	+
	ПК.29.В/ОУ з6. знать методы защиты информации от утечки по техническим каналам	+	+
	ПК.29.В/ОУ у2. уметь применять средства автоматического контроля, обнаружения и закрытия возможных каналов утечки защищаемых сведений	+	+

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

7. Литература

Основная литература

1. Ворона В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. - М., 2010. - 271 с., [1] л. ил. : ил., табл.

2. Волков А. М. Комплексная безопасность предприятий : учебное пособие / А. М. Волков, В. Н. Легкий, Ю. А. Попков ; Новосиб. гос. техн. ун-т. - Новосибирск, 2007. - 70, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000074126

3. Вернигоров Н. С. Особенности устройств съема информации и методы их блокировки : [учебное пособие] / Н. С. Вернигоров. - Томск, 2006. - 119 с. : ил.

4. Мельников В. П. Информационная безопасность и защита информации : [учебное пособие для вузов по специальности "Информационные системы и технологии"] / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М., 2011. - 330, [1] с. : ил., табл., схемы

Дополнительная литература

1. Малюк А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - М., 2005. - 144, [2] с.. - Библиогр.: с. 143-145.

2. Петраков А. В. Основы практической защиты информации. - М., 1999. - 368 с. : ил.

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. Соболев А. Н. Физические основы технических средств обеспечения информационной безопасности : [учебное пособие для вузов по специальностям 075500 "Комплексное обеспечение информационной безопасности автоматизированных систем" и 075200 "Компьютерная безопасность"] / А. Н. Соболев, В. М. Кириллов. - М., 2004. - 221, [2] с. : ил.

8.2 Специализированное программное обеспечение

1 Microsoft Windows

2 Microsoft Office

9. Материально-техническое обеспечение

Компьютерный класс

№	Наименование	Назначение
1	Терминальный класс №31	Сбор информационных материалов, получение навфков по оформлению документации.

Лабораторный стенд

№	Наименование	Назначение
1	Оборудование для лаборатории сигналов	Изучение схемотехники и принципов действия устройств съема информации и противодействия съему информации.

Специальное оборудование

№	Наименование	Назначение
1	Акустический сейф - Кокон	Получение навыков противодействия съему информации.
2	ПРИБОР D-008	Получение навыков поиска устройств съема информации.
3	ПОРТАТИВНЫЙ ОБНАРУЖИВАТЕЛЬ РПУ	Получение навыков поиска устройств съема информации.
4	СЕЛЕКТИВНЫЙ МИКРОВОЛЬТМЕТР 159	Получение навыков поиска устройств съема информации.
5	ТЕСТОВОЕ УСТРОЙСТВО PROTECT 1203	Получение навыков поиска устройств съема информации.

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

Кафедра автономных информационных и управляющих систем

“УТВЕРЖДАЮ”
ДЕКАН ФЛА
д.т.н., профессор С.Д. Саленко
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Методы противодействия техническим разведкам

Образовательная программа: 27.04.04 Управление в технических системах, магистерская программа: Автономные информационные и управляющие системы

Новосибирск 2017

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

Обобщенная структура фонда оценочных средств по **дисциплине** Методы противодействия техническим разведкам 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.29.В/ОУ способность соблюдать основные требования информационной безопасности	з4. знать возможные угрозы информационной безопасности	Определение основных понятий Передача информации по радиоканалу. Передача информации по телефонным линиям связи. Работа с кадрами Составление актов категорирования объекта вычислительной техники и акта классификации автоматизированной системы Средства и методы физической защиты объектов	РГЗ, разделы 1	Зачет, вопросы 1 - 14
ПК.29.В/ОУ	з5. знать технические мероприятия по защите информации	Законодательство РФ в области информационной безопасности Определение основных понятий Организация и обеспечение режима секретности Передача информации по радиоканалу. Понятие и виды защищаемой информации по законодательству РФ Составление технического паспорта на выделенное помещение Составление технического паспорта на объект вычислительной техники. Средства и методы физической защиты объектов	РГЗ, разделы 2	Зачет, вопросы 15 - 28
ПК.29.В/ОУ	з6. знать методы защиты информации от утечки по техническим каналам	Определение основных понятий Передача информации по радиоканалу. Передача информации по телефонным линиям связи. Понятие и виды защищаемой информации по законодательству РФ Работа с кадрами Составление актов категорирования объекта вычислительной техники и акта классификации автоматизированной системы Составление технического паспорта на выделенное помещение Средства и методы физической защиты объектов	РГЗ, разделы 3	Зачет, вопросы 29 - 42
ПК.29.В/ОУ	у2. уметь применять средства автоматического контроля, обнаружения и закрытия возможных каналов утечки защищаемых	Законодательство РФ в области информационной безопасности Организация и обеспечение режима секретности Передача информации по радиоканалу. Передача информации по телефонным линиям связи.	РГЗ, разделы 4	Зачет, вопросы 43 - 57

	сведений	Составление актов категорирования объекта вычислительной техники и акта классификации автоматизированной системы Составление технического паспорта на выделенное помещение Составление технического паспорта на объект вычислительной техники. Средства и методы физической защиты объектов		

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 2 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ПК.29.В/ОУ.

Зачет проводится в устной форме, по билетам.

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

В 2 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (РГЗ). Требования к выполнению РГЗ, состав и правила оценки сформулированы в паспорте РГЗ.

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 ПК.29.В/ОУ, 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.

Контролирующие материалы для аттестации студентов по дисциплине
Методы противодействия техническим разведкам

Вопросы к зачету:

1. Действующее в РФ законодательство в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.
2. Конституционные гарантии прав граждан на информацию и механизм их реализации.
3. Основные виды и особенности информации, её источники и носители.
4. Понятия и виды защищаемой информации по законодательству РФ.
5. Коммерческая тайна, как вид защищаемой информации по законодательству РФ.
6. Конфиденциальная информация и информация ограниченного доступа из её состава.
7. Существующие методы защиты сведений, составляющих коммерческую тайну.
8. Основные положения правового регулирования взаимоотношений администрации и персонала в области защиты информации.
9. Основные требования, на которых должны строиться взаимоотношения администрации и персонала в области защиты информации.
10. Международное законодательство в области защиты информации.
11. Компьютерные преступления. Виды, характеристика и законодательство по борьбе с ними.
12. Система защиты интеллектуальной собственности в РФ.
13. Правовые основы защиты информации с использованием различных средств защиты объектов информатизации от технических разведок.
14. Существующие потенциальные угрозы безопасности информации объектов и возможные пути их проявления.
15. Возможные пути реализации угроз безопасности информации объекта. (Методы доступа к информации).
16. Оценка ущерба вследствие противоправного выхода сведений ограниченного доступа из защищаемой сферы.
17. Меры по снижению ущерба (локализации потерь) от возможной утраты информации ограниченного доступа (типовые способы и средства предотвращения угроз).
18. Методы и средства реализации физической защиты объектов и их характеристика.
19. Средства, на основе которых реализуется подсистема физической (инженерной) защиты объектов.
20. Средства оповещения, входящие в состав системы инженерно-технической защиты.
21. Система видеонаблюдения, входящая в состав системы инженерно-технической защиты объектов.

22. Система контроля доступа, входящая в состав системы инженерно-технической защиты объектов.

23. Основные задачи, решаемые службой безопасности объекта.

24. Основные функции, выполняемые службой безопасности объекта.

25. Основные требования, которыми надлежит руководствоваться при формировании службы безопасности объекта, её возможная структура и решаемые подразделениями этой структуры задачи.

26. Подбор, прием, увольнение, расстановка кадров с учетом выявленных особенностей характера и поведения сотрудников в коллективе.

27. Работа с кадрами. Направленность кадровой политики администрации.

28. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну (документы, работы, образцы). Действующие в отношении этих лиц ограничения и компенсации.

29. Защита информации в экстремальных ситуациях и в условиях чрезвычайного положения (Типичные ситуации, при которых они возникают и сопровождающие их внешние и внутренние воздействующие на защищаемую информацию факторы).

30. Планируемые мероприятия и комплекс мер, позволяющих добиться минимизации последствий потерь от чрезвычайных положений.

31. Меры, реализация которых позволяет исключить возможность несанкционированного проникновения на территорию охраняемого объекта (в локальные зоны и помещения).

32. Технологические меры поддержания информационной безопасности объектов.

33. Организация режима охраны объектов в процессе транспортирования.

34. Обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного технического и экономического сотрудничества.

35. Информационное скрытие. (Решаемые задачи, способы и средства реализации).

36. Энергетическое скрытие. (Решаемые задачи, методы и средства реализации).

37. Структура и состав автономной системы охранно-пожарной сигнализации.

38. Контактные датчики (извещатели). (Виды и принцип работы электроконтактных датчиков).

39. Контактные датчики (извещатели). (Виды и принцип работы магнитоконтактных датчиков).

40. Контактные датчики (извещатели). (Виды и принцип работы удароконтактных датчиков).

41. Контактные датчики (извещатели). (Виды и принцип работы обрывных датчиков).

42. Акустические датчики (извещатели).(Виды и принцип работы этих датчиков в диапазоне звуковых волн).

43. Акустические датчики (извещатели). (Виды и принцип работы этих датчиков в диапазоне ультразвуковых волн).

44. Оптико-электронные датчики (извещатели). (Виды и принцип работы).

45. Микроволновые (радиоволновые) датчики (извещатели). (Виды и принцип работы радиолучевых датчиков).

46. Микроволновые (радиоволновые) датчики (извещатели). (Виды и принцип работы объемных и радиотехнических датчиков).

47. Вибрационные датчики (извещатели). (Виды и принцип их работы).

48. Емкостные датчики (извещатели). (Виды и принцип их работы).

49. Тепловые датчики (извещатели). (Виды и принцип их работы).

50. Ионизационные датчики (извещатели). Виды и принцип их работы.

51. Комбинированные датчики (извещатели). Цели и задачи, решаемые указанными датчиками.

52. Виды биометрических идентификаторов доступа на территорию охраняемого объекта (в локальную зону) и принцип их работы.

53. Назначение и состав основных технических средств и систем (ОТСС). Требования, предъявляемые к режиму их эксплуатации при работах с информацией, подлежащей защите.

54. Назначение и состав вспомогательных технических средств и систем (ВТСС). Требования, предъявляемые к режиму их эксплуатации при работах с информацией, подлежащей защите.

55. Физическая природа возникновения ПЭМИН. Технические средства, используемые при работе с защищаемой информацией, в которых возможно возникновение ПЭМИН. Действующие нормативные требования для оценки защищенности объектов информатизации, используемых для работы с конфиденциальной информацией.

56. Физическая природа возникновения явления электроакустопреобразований, возникающих в ВТСС. Действующие нормативные требования для оценки защищенности защищаемых помещений от утечки речевой информации при возникновении указанного явления.

57. Назначение защищаемого помещения (ЗП) и действующие нормативные требования для оценки уровня достаточности его защиты.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра автономных информационных и управляющих систем

Паспорт зачета

по дисциплине «Методы противодействия техническим разведкам», 2 семестр

1. Методика оценки

Зачет проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов _1 - 28_, второй вопрос из диапазона вопросов _29 - 57_ (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет ФЛА

Билет № _____
к зачету по дисциплине «Методы противодействия техническим разведкам»

---

1. Основные требования, которыми надлежит руководствоваться при формировании службы безопасности объекта, её возможная структура и решаемые подразделениями этой структуры задачи.
2. Назначение и состав основных технических средств и систем (ОТСС). Требования, предъявляемые к режиму их эксплуатации при работах с информацией, подлежащей защите.

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

2. Критерии оценки

• Ответ на билет для зачета считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать владение информацией по предмету, в пояснениях допускает принципиальные ошибки, оценка составляет *5 баллов.*

• Ответ на билет для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определения основных понятий, не способен показать уверенное владение информацией по предмету, в пояснениях допускает не принципиальные ошибки, оценка составляет *10 баллов*.

• Ответ на билет для зачета засчитывается на **базовом** уровне, если студент при ответе на вопросы дает определения основных понятий, способен показать уверенное владение

информацией по предмету, в пояснениях не допускает принципиальных ошибок, оценка оставляет *15 баллов.*

• Ответ на билет для зачета засчитывается на **продвинутом** уровне, если студент при ответе на вопросы дает определения основных понятий, способен показать уверенное владение информацией по предмету, в пояснениях не допускает принципиальных ошибок, способен привести несколько различных вариантов
правильных ответов, оценка оставляет *20 баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее _10__ баллов (из _20_ возможных).

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

Оценка знаний и умений студентов проводится в соответствии с «Положением о балльно-рейтинговой системе оценки достижений студентов НГТУ» от 02.07.09 г.

Рейтинг студента по дисциплине определяется как сумма баллов за работу в семестре (текущая аттестация) и баллов, полученных в результате итоговой аттестации (зачет)

Итоговая аттестация студента проводится в форме зачета. Максимальное количество баллов, которое студент может получить на зачете, равно **20.**

Общее количество баллов за виды учебной деятельности студента, предусмотренные программой освоения дисциплины, может составлять не более **80 баллов.**

Для получения допуска к зачету студент обязан выполнить все предусмотренные в рабочей программе дисциплины виды работ в семестре и набрать количество баллов не ниже минимально допустимого - **40 баллов**. Если по результатам работы в семестре студент набрал менее **25 баллов**, ему выставляется итоговая оценка по дисциплине «неудовлетворительно» (**F**) без права последующей пересдачи. В этом случае студенту предлагается изучить дисциплину повторно на платной основе. Если по результатам работы в семестре студент набрал **25 - 39 баллов,** то решение о допуске к сдаче зачета принимает декан факультета.

Если студенту выставляется итоговая оценка по дисциплине «неудовлетворительно» (**FX**) с правом последующей пересдачи, то в результате пересдачи студент имеет право получить оценку не выше (**E**).

Если студент в течение семестра в соответствии с установленными правилами аттестации по дисциплине набирает **80** баллов, то он вправе получить итоговую оценку «зачтено» и соответствующую оценку по 15-уровневой шкале ECTS без проведения процедуры итоговой аттестации.

Количество выставляемых баллов зависит от полноты и качества выполнения учебных заданий, своевременности сдачи работ.

В таблице 1 приводятся требования к текущей аттестации по дисциплине, формы контроля, минимальное и максимальное количество баллов по каждому виду деятельности.

Таблица 1

Формы контроля	**Требования к аттестации**	**Количество баллов**	
		Минимальное	**Максимальное**
Посещаемость лекционных и практических занятий	Пропуск занятия - 0 баллов Посещение занятия - 1 балл	**9**	**18**

Письменная проверочная работа на 5 минут по теме предыдущих лекционных занятий В семестре 5 работ.	В билете 2 вопроса (определение, формула, вопрос с вариантами ответа). Правильный ответ - 4,7 балла. Неточный ответ - 2,6 балла	за работу	за все работы	за работу	за все работы
		5,2	**26**	9,4	**47**
Расчетно-графическое задание, реферат	Оценка «отлично»: работа высокого качества, уровень выполнения отвечает всем	**5**		**15**	
Итоговое количество баллов за семестр		**40**		**80**	

Итоговая аттестация студента проводится в форме зачета. Оценка знаний и умений студентов проводится с помощью вопросов по основным проблемам дисциплины. Для оценки деятельности студента используются зачетные задания в виде 2-х теоретических вопросов. Теоретические вопросы формулируются в строгом соответствии с темами лекционных занятий. Максимальное количество баллов, которое студент может получить на зачете, равно **20**

Устанавливаются следующие правила аттестации студента (таблица 2).

Таблица 2

Характер ответа	**Количество баллов за ответ**
Правильный ответ на вопрос	10
Неполный ответ на вопрос	5 - 9
Неточный ответ на вопрос	1 - 4

Рейтинг студента для выставления итоговой оценки по дисциплине в «буквенной» форме в соответствии с 15-уровневой шкалой оценок ECTS, а также в традиционной форме приведен в таблице 3.

Таблица 3

Диапазон баллов рейтинга		**оценка ECTS**	**традиционная форма**
90-100	98 - 100	A+	ЗАЧТЕНО
	93 - 97	A	ЗАЧТЕНО
	90 - 92	A-	ЗАЧТЕНО
80-89	87 - 89	B+	ЗАЧТЕНО
	83 - 86	B	ЗАЧТЕНО
	80 - 82	B-	ЗАЧТЕНО
70-79	77 - 79	C+	ЗАЧТЕНО
	73 - 76	C	ЗАЧТЕНО
	70 - 72	C-	ЗАЧТЕНО
60-69	67 - 69	D+	ЗАЧТЕНО
	63 - 66	D	ЗАЧТЕНО
	60 - 62	D-	ЗАЧТЕНО
50-59		E	ЗАЧТЕНО
25-49		FX	НЕ ЗАЧТЕНО
0-24		F	НЕ ЗАЧТЕНО

4. Вопросы к зачету по дисциплине «Методы противодействия техническим разведкам»

1. Действующее в РФ законодательство в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.
2. Конституционные гарантии прав граждан на информацию и механизм их реализации.
3. Основные виды и особенности информации, её источники и носители.
4. Понятия и виды защищаемой информации по законодательству РФ.
5. Коммерческая тайна, как вид защищаемой информации по законодательству РФ.
6. Конфиденциальная информация и информация ограниченного доступа из её состава.
7. Существующие методы защиты сведений, составляющих коммерческую тайну.
8. Основные положения правового регулирования взаимоотношений администрации и персонала в области защиты информации.
9. Основные требования, на которых должны строиться взаимоотношения администрации и персонала в области защиты информации.
10. Международное законодательство в области защиты информации.
11. Компьютерные преступления. Виды, характеристика и законодательство по борьбе с ними.
12. Система защиты интеллектуальной собственности в РФ.
13. Правовые основы защиты информации с использованием различных средств защиты объектов информатизации от технических разведок.
14. Существующие потенциальные угрозы безопасности информации объектов и возможные пути их проявления.
15. Возможные пути реализации угроз безопасности информации объекта. (Методы доступа к информации).
16. Оценка ущерба вследствие противоправного выхода сведений ограниченного доступа из защищаемой сферы.
17. Меры по снижению ущерба (локализации потерь) от возможной утраты информации ограниченного доступа (типовые способы и средства предотвращения угроз).
18. Методы и средства реализации физической защиты объектов и их характеристика.
19. Средства, на основе которых реализуется подсистема физической (инженерной) защиты объектов.
20. Средства оповещения, входящие в состав системы инженерно-технической защиты.
21. Система видеонаблюдения, входящая в состав системы инженерно-технической защиты объектов.
22. Система контроля доступа, входящая в состав системы инженерно-технической защиты объектов.
23. Основные задачи, решаемые службой безопасности объекта.
24. Основные функции, выполняемые службой безопасности объекта.
25. Основные требования, которыми надлежит руководствоваться при формировании службы безопасности объекта, её возможная структура и решаемые подразделениями этой структуры задачи.
26. Подбор, прием, увольнение, расстановка кадров с учетом выявленных особенностей характера и поведения сотрудников в коллективе.
27. Работа с кадрами. Направленность кадровой политики администрации.
28. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну (документы, работы, образцы). Действующие в отношении этих лиц ограничения и компенсации.
29. Защита информации в экстремальных ситуациях и в условиях чрезвычайного положения (Типичные ситуации, при которых они возникают и сопровождающие их внешние и внутренние воздействующие на защищаемую информацию факторы).
30. Планируемые мероприятия и комплекс мер, позволяющих добиться минимизации последствий потерь от чрезвычайных положений.

31. Меры, реализация которых позволяет исключить возможность несанкционированного проникновения на территорию охраняемого объекта (в локальные зоны и помещения).
32. Технологические меры поддержания информационной безопасности объектов.
33. Организация режима охраны объектов в процессе транспортирования.
34. Обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного технического и экономического сотрудничества.
35. Информационное скрытие. (Решаемые задачи, способы и средства реализации).
36. Энергетическое скрытие. (Решаемые задачи, методы и средства реализации).
37. Структура и состав автономной системы охранно-пожарной сигнализации.
38. Контактные датчики (извещатели). (Виды и принцип работы электроконтактных датчиков).
39. Контактные датчики (извещатели). (Виды и принцип работы магнитоконтактных датчиков).
40. Контактные датчики (извещатели). (Виды и принцип работы удароконтактных датчиков).
41. Контактные датчики (извещатели). (Виды и принцип работы обрывных датчиков).
42. Акустические датчики (извещатели).(Виды и принцип работы этих датчиков в диапазоне звуковых волн).
43. Акустические датчики (извещатели). (Виды и принцип работы этих датчиков в диапазоне ультразвуковых волн).
44. Оптико-электронные датчики (извещатели). (Виды и принцип работы).
45. Микроволновые (радиоволновые) датчики (извещатели). (Виды и принцип работы радиолучевых датчиков).
46. Микроволновые (радиоволновые) датчики (извещатели). (Виды и принцип работы объемных и радиотехнических датчиков).
47. Вибрационные датчики (извещатели). (Виды и принцип их работы).
48. Емкостные датчики (извещатели). (Виды и принцип их работы).
49. Тепловые датчики (извещатели). (Виды и принцип их работы).
50. Ионизационные датчики (извещатели). Виды и принцип их работы.
51. Комбинированные датчики (извещатели). Цели и задачи, решаемые указанными датчиками.
52. Виды биометрических идентификаторов доступа на территорию охраняемого объекта (в локальную зону) и принцип их работы.
53. Назначение и состав основных технических средств и систем (ОТСС). Требования, предъявляемые к режиму их эксплуатации при работах с информацией, подлежащей защите.
54. Назначение и состав вспомогательных технических средств и систем (ВТСС). Требования, предъявляемые к режиму их эксплуатации при работах с информацией, подлежащей защите.
55. Физическая природа возникновения ПЭМИН. Технические средства, используемые при работе с защищаемой информацией, в которых возможно возникновение ПЭМИН. Действующие нормативные требования для оценки защищенности объектов информатизации, используемых для работы с конфиденциальной информацией.
56. Физическая природа возникновения явления электроакустопреобразований, возникающих в ВТСС. Действующие нормативные требования для оценки защищенности защищаемых помещений от утечки речевой информации при возникновении указанного явления.
57. Назначение защищаемого помещения (ЗП) и действующие нормативные требования для оценки уровня достаточности его защиты.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра автономных информационных и управляющих систем

Паспорт
расчетно-графического задания

по дисциплине «Методы противодействия техническим разведкам», 8 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты изучить каналы утечки информации и меры противодействия потере информации и материальных ценностей.

При выполнении расчетно-графического задания студенты должны провести анализ текущей ситуации рассматриваемого вопроса разработать алгоритм противодействия, выбрать аппаратные средства.

Обязательные структурные части РГЗ. 1. Введение (рассмотрение текущего состояния вопроса). 2. Построение модели нарушителя (определение канала утечки). 3. Построение модели противодействия (разработка аппаратно-административных мет противодействия утечке информации). 4. Определение эффективности проведенных мереприятий.

Оцениваемые позиции: Оценивается качество и полнота выполнения каждой составной части РГЗ и всей работы в целом.

2. Критерии оценки.

• Работа считается **не выполненной,** если выполнены не все части РГЗ, отсутствуют 2е и более либо выполнена всего одна обязательная структурная часть, оценка составляет 2 балла.

• Работа считается выполненной **на пороговом** уровне, если выполнены не все части РГЗ, отсутствуют не более одной обязательной структурной части и остальные выполнены формально (присутствуют недочеты, при защите студент путается в терминах и определениях), оценка составляет 5 баллов.

• Работа считается выполненной **на базовом** уровне, если выполнены все части РГЗ, не более одной обязательной части выполнено формально (присутствуют недочеты, при защите студент путается в терминах и определениях), оценка составляет 10 баллов.

• Работа считается выполненной **на продвинутом** уровне, если выполнены все части РГЗ, все обязательной части выполнено без замечаний (недочеты в работе отсутствуют, при защите студент уверен в терминах и определениях), оценка составляет 15 баллов.

3. Шкала оценки

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

4. Примерный перечень тем РГЗ

1. Разработка предложений по защите конфиденциальной речевой информации от съёма с волоконно-оптических линий связи.

2. Разработка программно-аппаратного комплекса по изучению характеристик и методов маскирования речевых сигналов.

3. Разработка предложений по выбору технических средств системы контроля и управления доступом для защиты информации предприятия.

4. Разработка предложений по инженерно-технической защите информации предприятия с распределенной территориальной структурой.

5. Разработка предложений по защите данных в PLC-сетях.

6. Разработка метода защиты графических изображений от встраивания вредоносной информации стеганографическими средствами.

7. Разработка методики защиты персональных данных на предприятии и ее реализация.

8. Разработка методики анализа защищенности СУБД систем электронного документооборота от SQL-инъекций.

9. Разработка демонстрационной модели волоконного акустооптического технического канала утечки информации.

10. Разработка анализатора настроек безопасности узлов локальной сети.

11. Разработка метода низкоуровневого контроля целостности системных файлов.

12. Разработка способа защиты информации для доступа в компьютерную систему от утечки по оптическому каналу.

13. Построение системы контроля физического доступа посторонних лиц с помощью средств охранного телевидения.

14. Разработка модуля обнаружения вредоносного программного обеспечения в сетевом трафике по сигнатурам.

15. Разработка способа обнаружения и противодействия атакам типа ARP-spoofing.

16. Разработка предложений по использованию протоколов обеспечения анонимности абонентов связи в компьютерных сетях.

17. Разработка модели резервного комплекса для управления банком в кризисных ситуациях.

18. Разработка утилиты обфускации программ, написанных на скриптовых языках.

19. Разработка метода и программного средства деобфускации обфусцированных программ.

20. Разработка предложений по защите корпоративной сети на основе межсетевого экранирования.

21. Разработка предложений по проведению аудита информационной безопасности информационно-вычислительных систем организаций финансово-кредитной сферы.

22. Разработка предложений по защите мультимедийной продукции от несанкционированного копирования.

23. Разработка модуля оценки соответствия балансировщика нагрузки BIG-IP требованиям безопасности.

24. Разработка механизмов защиты информационного портала для органов государственной власти.

25. Автоматизация исследований защищенности объекта информатизации от утечки по каналам акустоэлектрических преобразователей.

26. Организация спецпроверок защищаемого помещения с использованием нелинейных радиолокаторов.

27. Разработка предложений по организации защиты конфиденциальных переговоров в необорудованном помещении.

28. Анализ способов оценки защищенности автоматизированных систем в соответствии с документами ФСТЭК России.

29. Сравнительный анализ протоколов, используемых для построения защищенных (частных) виртуальных сетей (VPN).

30. Моделирование защищенных (частных) виртуальных сетей с помощью программы Cisco Packet Tracer.

31. Сравнительный анализ систем обнаружения и предотвращения компьютерных атак.

32. Моделирование процессов межсетевого экранирования локальной вычислительной сети с помощью программы Cisco Packet Tracer.

33. Оценка защищенности межсетевых экранов в соответствии с документами ФСТЭК России.

34. Анализ угроз атак на клиентов в автоматизированных системах и методов противодействия им.

35. Моделирование процессов защиты в локальной вычислительной сети организации с внешним доступом в сеть Интернет.

36. Разработка предложений по противодействию деструктивным информационным воздействиям в социальных сетях.

37. Разработка предложений по контент-анализу данных социальных сетей.

38. Разработка многополосной шкалы для анализа тональности текстов в задачах информационной безопасности.