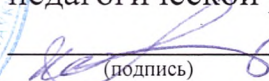


ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»



УТВЕРЖДАЮ:

Проректор по научно-
педагогической работе

 А.В. Мившов
(подпись) И.О. Фамилия

« 03 » 07 20 17 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Проектирование систем защиты информации»

(наименование дисциплины согласно учебному плану)

Направление (специальность)
подготовки:

10.03.01 «Информационная безопасность»

(код и наименование направления / специальности)

Направленность:

Информационная безопасность

(наименование профиля / магистерской программы / специализации)

Уровень образования:

бакалавриат

(бакалавриат, магистратура, специалитет)

Форма обучения:

очная

(очная, заочная, очно-заочная)

Семестры	7	8
Общая трудоёмкость в з.е./часах	3,5/126	3,0/108
Аудиторные занятия (час.), в том числе	51	56
Лекции (час.)	34	24
Практические (семинарские) занятия (час.)	-	16
Лабораторные работы (час.)	17	16
Самостоятельная работа (час.), в том числе	39	52
Курсовой проект/работа (сем/кол.)	-	-
Индивидуальное задание (сем/кол.)	-	-
Форма промежуточной аттестации (экзамен/зачёт):	Экзамен	Зачет

Донецк, 2017 г.

Рабочая программа дисциплины «Проектирование систем защиты информации» составлена в соответствии с учебным планом по направлению подготовки 10.03.01 – «Информационная безопасность» для 2017 года приёма.

Составитель: Фунтиков М.Н., старший преподаватель кафедры радиотехники и защиты информации

Рабочая программа **рассмотрена и утверждена** на заседании кафедры радиотехники и защиты информации.

Протокол от « 25 » 05 20 17 года № 10

Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Рабочая программа **согласована с выпускающей кафедрой** радиотехники и защиты информации.

Протокол от « 25 » 05 20 17 года № 10

Заведующий кафедрой _____ (Паслён В.В.)
(подпись) (Ф.И.О.)

Рабочая программа одобрена учебно-методической комиссией ДонНТУ по направлению подготовки 10.03.01 – «Информационная безопасность».

Протокол от « 30 » 06 20 17 года № 11

Председатель _____ (Паслён В.В.)
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20 18 года приёма на заседании кафедры радиотехники и защиты информации.

Протокол от « 31 » 08 20 18 года № 1

Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Согласовано с выпускающей кафедрой радиотехники и защиты информации.

Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20 19 года приёма на заседании кафедры радиотехники и защиты информации.

Протокол от « 28 » 08 20 19 года № 1

Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Согласовано с выпускающей кафедрой радиотехники и защиты информации.

Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20 ____ года приёма на заседании кафедры радиотехники и защиты информации.

Протокол от « ____ » ____ 20 ____ года № ____

Заведующий кафедрой _____
(подпись) (Ф.И.О.)

Согласовано с выпускающей кафедрой радиотехники и защиты информации.

Заведующий кафедрой _____
(подпись) (Ф.И.О.)

1 ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина рассматривает вопросы теоретико-методологических основ проектной деятельности; анализа и обоснования выбора решений по обеспечению требуемого уровня эффективности применения автоматизированных систем; управления информационной безопасностью автоматизированной системы; применения и внедрения программных, программно-аппаратных и технических методов и средств защиты информации в распределенных автоматизированных и информационно-управляющих системах.

Целью дисциплины является: формирование у студентов научных знаний и понимания теоретических основ проектной деятельности; компетенций в разработке компонентов автоматизированных систем в профессиональной деятельности; теоретическая и практическая подготовка специалистов к деятельности, связанной с разработкой и эксплуатацией защищенных автоматизированных систем в своей профессиональной деятельности.

В результате освоения дисциплины студент должен:

Знать: содержание основных этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; правила безопасной и технической эксплуатации электроустановок; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; основные меры технической защите информации в автоматизированных системах; основные нормативно-правовые и санитарно-эпидемиологические документы в области использования радиоэлектронных и информационных систем; организационно-технические мероприятия по восстановлению работоспособности систем защиты информации при возникновении нештатных ситуаций; основные современные методы и технологии по обеспечению безопасности информации.

Уметь: применять методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем; применять государственные и международные стандарты, связанные с профессиональной деятельностью; разрабатывать предложения по совершенствованию мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности в автоматизированных и информационно-управляющих системах; проектировать комплексные защищенные автоматизированные системы.

Владеть: основными методами анализа и приемами обоснования технологического решения по обеспечению требуемого уровня эффективности автоматизированных систем; технологиями проведения экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации; основными приемами управления информационной безопасностью автоматизированной системы; методами проведения оценки эффективности средств защиты информации.

Процесс изучения дисциплины направлен на формирование следующих компетенций: способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления (ОК-7); способность к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства (ОК-10); способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ОПК-1); способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ОПК-2); способность использовать нормативные правовые документы в своей профессиональной деятельности (ОПК-3); способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ОПК-4); способность организовывать и поддерживать выполнение комплекса мер по информационной

безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ОПК-5); способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ОПК-6); способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-1); способность администрировать подсистемы информационной безопасности объекта (ПК-2); способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-3); способность участвовать в разработке подсистемы управления информационной безопасностью (ПК-4); способность использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-8); способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-10); способность применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-12); способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-13); способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов (ПК-14); способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-16); способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-18); способность организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами (ПК-25).

2 МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина «Проектирование систем защиты информации» относится к циклу профессиональной и практической подготовки вариативной части учебного плана по выбору вуза; базируется на знаниях и умениях, которые студент приобрел при освоении предшествующих дисциплин: «Физика», «Информационные технологии», «Высшая математика», «Основы теории цепей, сигналов и процессов», «Поля и волны в системах технической защиты информации», «Схемотехника устройств технической защиты информации». Знания и умения, приобретенные при освоении данной дисциплины, реализуются студентом при прохождении производственной практики.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Распределение учебных часов по темам дисциплины и видам занятий

Наименование тем (содержательных модулей)	Количество часов				
	Всего	в том числе			
		лекции	практ.	лабор.	СРС
7-й семестр					
Тема 1. Общие основы проектирования и конструирования	6	4	-	-	2
Тема 2. Классификация электроустановок	15	6	-	4	5
Тема 3. Категории электроприемников и обеспечение надежности электроснабжения	20	6	-	4	10
Тема 4. Правила безопасной технической эксплуа-	15	6	-	4	5

тации электроустановок					
Тема 5. Электромагнитные поля в производственных условиях	21	6	-	5	10
Тема 6. Этапы разработки проектно-конструкторской документации	13	6	-	-	7
Итого по 7-му семестру:	90	34	-	17	39
8-й семестр					
Тема 7. Основные принципы проектирования систем технической защиты информации	10	2	-	-	8
Тема 8. Требования по проектированию аппаратных помещений	18	4	4	4	6
Тема 9. Проектирование аппаратных помещений с общим доступом	14	4	2	2	6
Тема 10. Проектирование аппаратных помещений с разграничением доступа	14	2	2	2	8
Тема 11. Классификация угроз информационной безопасности. Методы и модели оценки уязвимостей	16	4	-	2	10
Тема 12. Классификация каналов проникновения в систему. Утечка информации	18	4	4	4	6
Тема 13. Характеристики нежелательных электромагнитных связей, излучений радиопередающих устройств, технических средств обработки информации.	18	4	4	2	8
Итого по 8-му семестру:	108	24	16	16	52
ВСЕГО	198	58	16	33	91

3.2 Лекции

Тема 1. Общие основы проектирования и конструирования

- 4 часа

Содержание темы 1:

Предмет, задачи, функции проектирования систем защиты информации. Основные категории проектирования и конструирования. Практическое применение знаний принципов проектирования в профессиональной деятельности инженера.

Литература к теме 1: [4]

Тема 2. Классификация электроустановок

- 6 часов

Содержание темы 2:

Классификация электроустановок. Правила устройства электроустановок.

Литература к теме 2: [14, 15]

Тема 3. Категории электроприемников и обеспечение надежности

электрооборудования

- 6 часов

Содержание темы 3:

Категории электроприемников и обеспечение надежности электрооборудования. Защитное заземление. Типология стандартов систем заземления. Утечка информации по цепям заземления.

Литература к теме 3: [14, 15]

Тема 4. Правила безопасной технической эксплуатации электроустановок

- 6 часов

Содержание темы 4:

Организационные мероприятия для безопасного проведения электротехнических работ. Технические мероприятия для безопасного проведения электротехнических работ.

Литература к теме 4: [14, 15]

Тема 5. Электромагнитные поля в производственных условиях - 6 часов

Содержание темы 5:

Электромагнитные поля в производственных условиях. Требования к проведению контроля электромагнитных полей в радиочастотном диапазоне. Принципы и методы контроля. Требования к коллективным и индивидуальным средствам защиты при воздействии электромагнитных полей в производственных условиях.

Литература к теме 5: [11, 12, 13, 16]

Тема 6. Этапы разработки проектно-конструкторской документации - 6 часов

Содержание темы 6:

Разработка конструкторской документации. Научно-исследовательские и опытно-конструкторские работы. Типовые стандарты и положения, регламентирующие разработку технического задания, технического предложения, эскизного проектирования, технического проектирования, рабочей конструкторской документации. Требования к надёжности проектируемых технических систем.

Литература к теме 6:[4, 18]

Тема 7. Основные принципы проектирования систем технической защиты информации - 2 часа

Содержание темы 7:

Основные принципы организации систем технической защиты информации. Основные этапы работы по созданию систем технической защиты информации. Классификация объектов защиты информации.

Литература к теме 7: [12, 13]

Тема 8. Требования по проектированию аппаратных помещений - 4 часа

Содержание темы 8:

Основные требования по проектированию аппаратных помещений. Требования к размещению оборудования и коммуникационных каналов при проектировании аппаратных помещений. Требования к подсистемам при проектировании аппаратных помещений.

Литература к теме 8: [13, 16]

Тема 9. Проектирование аппаратных помещений с общим доступом - 4 часа

Содержание темы 9:

Проектирование аппаратных помещений с общим доступом. Требования по пожарной безопасности при проектировании аппаратных помещений с общим доступом. Требования по электроснабжению при проектировании аппаратных помещений с общим доступом.

Литература к теме 9: [13, 16]

Тема 10. Проектирование аппаратных помещений с разграничением доступа - 2 часа

Содержание темы 10:

Проектирование аппаратных помещений с разграничением доступа. Принципы технической реализации разграничения доступа при проектировании аппаратных помещений.

Литература к теме 10: [13, 16]

Тема 11. Классификация угроз информационной безопасности.

Методы и модели оценки уязвимостей.

- 4 часа

Содержание темы 11:

Распределённые автоматизированные системы. Характеристики основных уязвимостей. Классификация угроз информационной безопасности. Методы и модели оценки уязвимостей.

Литература к теме 11: [5, 21]

Тема 12. Классификация каналов проникновения в систему. Утечка информации -4 часа

Содержание темы 12:

Классификация каналов проникновения в систему. Методы несанкционированного доступа. Высокочастотное зондирование. Защита информации от высокочастотного навязывания.

Литература к теме 12: [5, 21]

Тема 13. Характеристики нежелательных электромагнитных связей, излучений радиопередающих устройств, технических средств обработки информации - 4 часа

Содержание темы 13:

Характеристики нежелательных излучений радиопередающих устройств. Характеристики нежелательных электромагнитных связей. Характеристики нежелательных излучений технических средств обработки информации. Случайные излучающие антенны.

Литература к теме 13: [19, 20]

3.3 Практические занятия

№ п/п	Тема занятия	Объем, час.
8-й семестр		
1	Требования по проектированию аппаратных помещений	4
2	Проектирование аппаратных помещений с общим доступом	2
3	Проектирование аппаратных помещений с разграничением доступа	2
4	Классификация угроз информационной безопасности. Методы и модели оценки уязвимостей	2
5	Классификация каналов проникновения в систему. Утечка информации	4
6	Характеристики нежелательных электромагнитных связей, излучений радиопередающих устройств, технических средств обработки информации. Случайные излучающие антенны	2
Итого:		16

3.4 Лабораторные работы

№ п/п	Название работы	Объем, час.
7-й семестр		
1	Выявление источников и носителей информации на промышленном предприятии	4
2	Выявление и анализ угроз безопасности информации в документообороте предприятия	4
3	Подбор технических средств для обеспечения защиты информации	4

4	Анализ рисков безопасности информации	5
Итого:		17
8-й семестр		
1	Проектирование автоматизированных рабочих мест в помещении с общим уровнем доступа	4
2	Проектирование «серверной» станции в помещении с ограниченным уровнем доступа	4
3	Проектирование автоматизированных рабочих мест в помещении с секретным уровнем доступа	4
4	Проектирование системы видеонаблюдения в специализированной виртуальной среде VideoCAD	4
Итого:		16
Всего		33

3.5 Самостоятельная работа студента

№ п/п	Виды самостоятельной работы студента	Объем, час.	
		7-й семестр	8-й семестр
1	Проработка теоретического материала	17	12
2	Подготовка к лабораторным работам	22	30
3	Подготовка к практическим занятиям	-	10
Итого:		39	52

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В процессе изучения дисциплины применяются следующие виды контроля:

1) Текущее тестирование или текущий опрос по изученным темам программы. Текущее тестирование или текущий опрос проводится во время лекционных, практических и лабораторных занятий, также учитывается качество и своевременность выполнения и сдачи соответствующей лабораторной работы.

2) Оценка качества и своевременность выполнения заданий, относящихся к соответствующей теме.

3) Промежуточная аттестация по результатам освоения дисциплины в семестре проводится в форме зачета в соответствии с «Положением об организации учебного процесса в Донецком национальном техническом университете (новая редакция)», утвержденном приказом ДонНТУ № 1006-14 от 01.12.2016 г.

Для определения уровня знаний студентов преподаватель руководствуется критериями оценки знаний, являющимися составляющей учебно-методического комплекса дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Рекомендуемая литература:

1. Хартов, В.Я. Микропроцессорные системы / В. Я. Хартов. - М.: ИЦ "Академия", 2010. - 352с. -10 экз.
2. Ревич, Ю.В. Практическое программирование микроконтроллеров Atmer AVR на языке ассемблера / Ю. В. Ревич. - СПб.: БХВ-Петербург, 2011. - 352с. – 1 экз.
3. Шеин, А.Б. Методы проектирования электронных устройств / А. Б. Шеин, Н. М. Лазарева. - М. : Инфра-Инженерия, 2011. - 456с. – 2 экз

4. Краснощекова Г.Ф. Особенности проектирования электронных средств специального назначения [Электронный ресурс] : научно-образовательный модуль / Г. Ф. Краснощекова (Нац. исследоват. ун-т). - 1 Мб. - Самара : [б.и.], 2012. - 1 файл.
5. Барсуков В.С. Особенности обеспечения информационной безопасности. – М.: ТЭК, 1996
6. В.А. Герасименко, А.А. Малюк Основы защиты информации М: ООО «Инкомбук», 1995
7. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ДиаСофт, 2002 – 511 с.
8. Домарев В.В. Безопасность информационных технологий. Системный подход. К.: ДиаСофт, 2000 – 460 с.
9. Защита информации и безопасность компьютерных систем / В.В. Домарев. - К.: ДиаСофт, 1999 – 984 с.
10. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия Телеком, 2000 – 311 с.
11. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.
12. Малюк А.А. Информационная безопасность: концептуальные и методические основы защиты информации. Учеб. пособие для вузов. – М: Горячая линия – Телеком, 2004. – 280 с. ил
13. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах – М.Ж Горячая линия-Телеком, 2001 – 156 с.
14. Правила безопасности при эксплуатации электроустановок – Минэнерго РФ, 2000.– 105с
15. Правила технической эксплуатации электроустановок потребителей – Минэнерго РФ, 2003. – 269 с.
16. Прокофьев И.В. Защита информации в информационных системах. – М.: Европейский центр по качеству, 2002 – 340 с.
17. Расторгуев С.П. Информационная война и Россия. – М.: Мир безопасности, 2000 – 127 с.

Дополнительная литература:

18. Алексеенко В.Н., Соколовский Б.В. Система защиты коммерческих объектов. Технические средства защиты. Практическое пособие для предпринимателей и руководителей служб безопасности. М., 1992 – 156 с.
19. Карпов Е.А., Котенко И.В., Боговик И.В. Основы теории управления в системах военного назначения. Часть II. Учебное пособие. – СПб.: ВУС, 2000 – 342 с.
20. Каторин Ю.Ф., Куренков Е.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. – СПб.: ООО «Издательство Полигон», 2000 – 280 с.
21. Торокин А.А. Основы инженерно-технической защиты информации. – М.: Ось-89, 1996 г. – 486 с.
22. Конспект лекций по дисциплине «Проектирование систем защиты информации». / Сост. Фунтиков М. Н. – Донецк.: ДонНТУ
- 23 Методические указания к выполнению лабораторных работ по дисциплине «Проектирование систем защиты информации» - Донецк: ДонНТУ.

Периодические издания

24. Радио (2008 - 2014)
- 25 Бизнес и безопасность (2014)
- 26 Автоматизация и современные технологии (2008-2013)
- 27 Прикладная информатика (2011, 2012) эл. ресурс

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

- учебная аудитория, оснащенная средствами воспроизведения мультимедийных технологий;
- компьютерный класс, с доступом к информационным ресурсам;
- обеспечение открытого доступа для студентов к электронным библиотекам и ресурсам по проблемам радиоэлектроники и технических средств защиты информации, интер-

нет-порталам, электронным архивам периодических изданий. Каждый студент обеспечен рабочим местом в компьютерном классе в соответствии с объемом дисциплины.

Составитель рабочей программы: _____ М.Н. Фунтиков