

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



УТВЕРЖДАЮ:

Проректор по научно-  
педагогической работе

(подпись)

И.О. Фамилия

« 03 » 07 20 17 года

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**«Методы и средства защиты информации»**

(наименование дисциплины согласно учебному плану)

Направление (специальность)  
подготовки:

11.03.01 «Радиотехника»

(код и наименование направления / специальности)

Направленность:

Радиотехника

(наименование профиля / магистерской программы / специализации)

Уровень образования:

бакалавриат

(бакалавриат, магистратура, специалитет)

Форма обучения:

очная

(очная, заочная, очно-заочная)

Семестры	5	6
Общая трудоёмкость в з.е./часах	2,0/72	2,5/90
Аудиторные занятия (час.), в том числе	34	51
Лекции (час.)	17	34
Практические (семинарские) занятия (час.)	-	-
Лабораторные работы (час.)	17	17
Самостоятельная работа (час.), в том числе	38	39
Курсовой проект/работа (сем/кол.)	-	-
Индивидуальное задание (сем/кол.)	1	1
Форма промежуточной аттестации (экзамен/зачёт):	Зачет	Зачет

Донецк, 2017 г.

Рабочая программа дисциплины «Методы и средства защиты информации» составлена в соответствии с учебным планом по направлению подготовки 11.03.01 – «Радиотехника» для 2017 года приёма

Составитель: Константинов С.В., к.т.н., доц. кафедры «Радиотехники и защиты информации»

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

Протокол от « 04 » 06 20 17 года № 10

Заведующий кафедрой \_\_\_\_\_ (Паслён В.В.)  
(подпись) (Ф.И.О.)

Рабочая программа **согласована с выпускающей кафедрой** Радиотехники и защиты информации:

Протокол от « 16 » 08.17 20 17 года № 10

Заведующий кафедрой \_\_\_\_\_ (Паслён В.В.)  
(подпись) (Ф.И.О.)

Рабочая программа **одобрена учебно-методической комиссией** ДонНТУ по направлению подготовки 11.03.01 – «Радиотехника»:

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 \_\_\_\_\_ (Паслён В.В.)  
(подпись) (Ф.И.О.)

Согласовано с выпускающей кафедрой Радиотехники и защиты информации:

Заведующий кафедрой \_\_\_\_\_ (Паслён В.В.)  
(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 \_\_\_\_\_ (Паслён В.В.)  
(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. ЦЕЛЬ И ЗАДАЧА УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью изучения дисциплины является сформировать у студентов знания и навыки по оценке возможностей злоумышленников по перехвату информации по техническим каналам; выполнению работ по исследованию характеристик средств защиты информации от утечки по техническим каналам; выполнения комплекса мер по защите объектов информатизации от утечки информации и информатизации от утечки информации по техническим каналам.

Задачами дисциплины является изучение понятийного аппарата дисциплины, основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения практических, профессиональных и/или прикладных задач.

**В результате изучения учебной дисциплины студент должен:**

**Знать:** цели и задачи защиты информации от утечки по техническим каналам; нормативно-методические документы по защите информации от утечки по техническим каналам; технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ), возможности специальных технических средств по перехвату информации, обрабатываемой СВТ; технические каналы утечки акустической (речевой) информации, возможности средств акустической (речевой) разведки по перехвату разговоров из выделенных помещений; принципы построения и основные характеристики средств защиты объектов информатизации от утечки информации по техническим каналам, основные характеристики этих средств; принципы построения и основные характеристики средств защиты выделенных помещений от утечки речевой информации по техническим каналам, основные характеристики этих средств; методы и средства контроля эффективности защиты СВТ от утечки информации по техническим каналам; методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам; методы и средств выявления электронных устройств перехвата информации; организацию защиты объектов информатизации от утечки информации по техническим каналам; организацию аттестации объектов информатизации и выделенных помещений по требованиям безопасности информации;

**Уметь:** проводить анализ потенциальных технических каналов утечки информации на объектах информатизации, рассчитывать опасные зоны К2, г1 и г2; проводить анализ потенциальных технических каналов утечки речевой информации в выделенных помещениях, рассчитывать словесную разборчивость речи; проводить экспериментальные исследования средств защиты информации от утечки по техническим каналам; разрабатывать предложения по созданию (модернизации) системы защиты объекта информатизации от утечки по техническим каналам; разрабатывать программу и методику аттестационных испытаний объектов информатизации по требованиям защиты информации от утечки по техническим каналам.

Перечисленные требования направлены на формирование следующих компетенций и видов профессиональной деятельности: способность к самоорганизации и самообразованию (ОК-7); способность выявлять естественно-научную сущность проблем, возникающих в ходе профессиональной деятельности, привлекать для их решения соответствующий физико-математический аппарат (ОПК-2); готовность применять современные средства выполнения и редактирования изображений и чертежей и подготовки конструкторско-технологической документации (ОПК-4); способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности (ОПК-9). способность выполнять математическое моделирование объектов и процессов по типовым методикам, в том числе с использованием стандартных пакетов прикладных программ (ПК-1); осуществлять сбор и анализ исходных данных для расчета и проектирования деталей, узлов и устройств радиотехнических систем (ПК-5); готовность выполнять расчет и проектирование деталей, узлов и устройств радиотехнических систем в соответствии с техническим заданием с использованием средств автоматизации проектирования (ПК-6); готовность внедрять результаты разработок в производство (ПК-9).

## 2. МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина «Методы и средства защиты информации» относится к профессиональному циклу дисциплин вариативной части выполнения учебного плана; базируется на знаниях и

умениях, которые студент приобрел при освоении материала базовой и вариативной частей учебного плана, а также на компетенциях бакалавра по освоению дисциплин общенаучного цикла.

Знания и умения, приобретенные при освоении данной дисциплины, реализуются студентом при освоении последующих дисциплин обучения и прохождении производственной и преддипломной 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	Лабор.	СРС
5-й семестр				
Тема 1. Введение Термины и определения. Угрозы для информации.	8	2	-	6
Тема 2. Физические основы и особенности образования технических каналов утечки информации.	8	2	3	3
Тема 3. Основные принципы технической защиты информации	9	2	4	3
Тема 4. Методы и средства защиты информации обрабатываемой ТСПИ от утечки по техническим каналам.	9	2	4	3
Тема 5. Технические каналы утечки при передаче информации по каналам связи	7	2	2	3
Тема 6. Характеристика технических каналов утечки информации	5	2	-	3
Тема 7. Средства перехвата информации с проводных линий связи	9	2	4	3
Тема 8. Технические средства добывания информации	5	2	-	3
Тема 9. Методы и средства контроля эффективности защиты информации	3	1	-	2
Итого по 5-му семестру:	63	17	17	29
6-й семестр				
Тема 10. Основы проектирования защиты объектов информатизации. Методы и средства поиска и нейтрализации несанкционированного съема информации.	7	4	-	3
Тема 11. Звукоизоляция помещений. Звукоизоляция коммуникаций. Генераторы шума.	9	6	-	3
Тема 12. Организационные мероприятия по защите информации	8	2	3	3
Тема 13. Технические каналы утечки при передаче информации по каналам связи	9	4	2	3
Тема 14. Методы и средства обнаружения и подавления диктофонов и акустических закладок	11	4	4	3
Тема 15. Методы и средства защиты телефонных (слаботочных) линий	11	4	4	3
Тема 16. Средства защиты информации за счет ПЭМИН	7	4	-	3

Тема 17. Экранированные помещения и кабины	9	2	4	3
Тема 18. Заземление.	5	2	-	3
Тема 19. Фильтрация	5	2	-	3
<b>Итого по 6-му семестру:</b>	<b>81</b>	<b>34</b>	<b>17</b>	<b>30</b>
<b>Всего:</b>	<b>144</b>	<b>51</b>	<b>34</b>	<b>59</b>

### 3.2. Лекции

#### *Лекция 1.* Введение Термины и определения. Угрозы для информации. (2 часа)

Системный подход к защите информации. Характеристика инженерно-технической защиты информации. Основные параметры системы защиты информации. Основные концептуальные положения инженерно-технической защиты информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.

Техническая защита информации, безопасность информации, конфиденциальность информации, *целостность* информации, доступность информации, угроза (безопасности информации), уязвимость (информационной системы), утечка (информации) по техническому каналу, перехват (информации), несанкционированное блокирование доступа к информации

Литература к лекции [1]

#### *Лекция 2.* Физические основы и особенности образования технических каналов утечки информации. (2 часа)

Понятие о каналах несанкционированного получения информации, причинах нарушения целостности информации и технических каналах утечки информации (ТКУИ). Классификация ТКУИ. Физические основы электромагнитных каналов утечки информации. Основные свойства электромагнитного поля, элементарные источники побочных электромагнитных излучений (ПЭМИ). Источники возникновения и характер помеховых электромагнитных излучений (ЭМИ). ЭМИ на частотах работы высокочастотных генераторов и на частотах самовозбуждения усилителей низкой чистоты (УНЧ).

Литература к лекции [1, 2]

#### *Лекция 3.* Основные принципы технической защиты информации (2 часа)

Методы инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов. Методы инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения.

Литература к лекции [1, 5]

#### *Лекция 4.* Методы и средства защиты информации, обрабатываемой ТСПИ от утечки по техническим каналам. (2 часа)

Пассивные методы защиты информации, обрабатываемой ТСПИ: экранирование технических средств, заземление технических средств, фильтрация информационных сигналов. Экологически чистые технологии пассивной защиты информации. Активные методы и средства защиты информации, обрабатываемой ТСПИ. Методы и средства пространственного и линейного зашумления.

Литература к лекции [1, 2]

#### *Лекция 5.* Технические каналы утечки при передаче информации по каналам связи (2 часа)

Распространение сигналов в технических каналах утечки информации. Распространение радиосигналов различных диапазонов в пространстве и направляющим линиям связи. Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе. Физические процессы подавления опасных сигналов.

Литература к лекции [1, 2]

#### *Лекция 6.* Характеристика технических каналов утечки информации (2 часа)

Перехват побочных электромагнитных излучений (ПЭМИ). побочные электромагнитные излучения, возникающие при обработке информации на ПК. Перехват ПЭМИ, возникающих вследствие паразитной генерации в элементах ТСПИ.

Литература к лекции [1]

**Лекция 7.** Утечка информации по техническим каналам. (2 часа)

Информация как предмет защиты. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Источники опасных сигналов. Основные и вспомогательные технические средства, и системы, их классификация и характеристика. Опасные сигналы, образующиеся в результате акустоэлектрических преобразований. Виды побочных опасных электромагнитных излучений. Паразитные связи и наводки опасных сигналов. Характеристика технической разведки. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки по добыванию разведывательной информации. Технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.

Литература к лекции [1]

**Лекция 8.** Технические средства добывания информации (2 часа)

Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного прослушивания. Автономные средства разведки. Средства инженерной защиты и технической охраны. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.

Литература к лекции [1, 4]

**Лекция 9.** Методы и средства контроля эффективности защиты информации. (2 часа)

Методы и средства контроля эффективности защиты информации от ее утечки по электромагнитным каналам. Измерительные антенны. Калибровка измерительных антенн. Методы и средства измерения параметров опасных сигналов в электромагнитном поле. Современные средства автоматизации измерений при спец исследованиях технических средств. Методы и средства оценивания эффективности защиты акустической информации от утечки по виброакустическим каналам с использованием инструментальных средств.

Литература к лекции [2]

**Лекция 10.** Основы проектирования защиты объектов информатизации. (2 часа)

(Понятие о моделировании объектов защиты информации. Проектирование защиты информации: определение требований к защите информации; анализ условий защиты информации; выявление возможных ТКУИ; оценивание защищенности информации от утечки по возможным ТКУИ; выбор средств защиты информации; документальное оформление проекта защиты информации. Разработка элементов проекта защиты информации на объекте информатизации.)

Литература к лекции [2]

**Лекция 11.** Методы и средства поиска и нейтрализации несанкционированного съема информации. (2 часа)

Методы и средства поиска с использованием индикаторов, радиочастотомеров. Сканирующие приемники и анализаторы спектра для поиска устройств перехвата информации. Программно-аппаратные комплекты радиоконтроля. Методы поиска устройств съема информации с использованием нелинейных локаторов, металлоискателей, рентгеновских аппаратов. Средства и методы контроля проводных линий. Специальные проверки служебных помещений. Программа организации работ.

Литература к лекции [1, 2]

**Лекция 12.** Звукоизоляция помещений. (2 часа)

Основные требования к звукоизоляции помещений. Архитектурные решения для звукоизоляции помещений. Звукопоглощение и звукоизоляция. Увеличение звукоизолирующей способности дверей. применение уплотняющих прокладок. Звукоизоляция окон.

**Лекция 13.** Звукоизоляция коммуникаций (2 часа)

Звукопоглощающие материалы и конструкции. Особенности применения звукопоглощающих материалов. Сплошные и пористые звукопоглощающие материалы. Облицовочные звукопоглощающие материалы. Сравнительные частотные характеристики звукоизоляции каркасных перегородок, звукоизолирующие крепления. Установка звукопоглощающего ограждения. Звукоизоляция отверстий и проемов для труб водоснабжения, отопления и т.д.

Литература к лекции [4]

**Лекция 14.** Генераторы шума. (2 часа)

Обобщенная функциональная схема цифрового генератора шума. «Белый» шум. «Розовый» шум. Шум с тенденцией спада спектральной плотности на 6 дБ на октаву. Шумовая «речеподобная» помеха Помехи, сформированные из скрываемого сигнала. Коэффициент качества шума. Виброизлучатели, виброизлучатели электромагнитного или пьезоэлектрического принципа действия. Достоинства недостатки. Эффективный радиус подавления виброизлучателя. Анализ среднего уровня вибрационного шумового сигнала.

Литература к лекции [4]

**Лекция 15.** Организационные мероприятия по защите информации (2 часа)

Система защиты сведений, отнесенных к коммерческой тайне. структура службы безопасности предприятия. обеспечение безопасности производственно-торговой деятельности, защита информации и сведений, являющихся коммерческой тайной; организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны; организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;

Литература к лекции [3]

**Лекция 16.** Технические каналы утечки при передаче информации по каналам связи (2 часа)

(Технический канал утечки при передаче информации по каналам связи. Основные виды электросвязи с помощью которых передается информация от одного абонента к другому. Технический канал утечки при передаче информации по каналам связи. Перехват информации, передаваемой по проводным линиям связи)

Литература к лекции [1, 4,]

**Лекция 17.** Перехват информации, передаваемой по волоконно-оптическим линиям связи (2 часа)

(Методы съёма информации Способы защиты Методы несанкционированного доступа Теоретическая основа Моды цилиндрического волновода Потери на изгибе волокна.)

Литература к лекции [1, 2]

**Лекция 18.** Методы и средства обнаружения диктофонов и акустических закладок (2 часа)

Обнаружение диктофонов; Обнаружение акустических закладок. Сложность задачи обнаружения современных диктофонов. Задачи обнаружителя. детекторы диктофонов. Характер создаваемого электромагнитного излучения. Конструктивно «цифровые» диктофоны. максимальный уровень излучения цифровых диктофонов. диктофоны с подключенным выносным микрофоном. диктофоны в металлических корпусах. Решение задачи обнаружения диктофонов. Структурная схема обнаружителя диктофонов. регистрация излучения диктофона.

Литература к лекции [4]

**Лекция 19.** Методы и средства подавления диктофонов и акустических закладок (2 часа)

Частотные характеристики типичного фонового излучения в условиях офиса. Размещение зон обнаружения (ближней) и зон (дальней) где источник излучения не обнаруживается. Собственный шум детектора диктофонов. Виды подавления диктофонов. Стационарные комплексы подавления. Переносные комплексы подавления.

Литература к лекции [6, 7]

**Лекция 20.** Методы и средства защиты телефонных (слаботочных) линий (2 часа)

Методы и средства защиты телефонных (слаботочных) линий от утечки информации за счет акустоэлектрических преобразований; Пассивные методы защиты. Активные методы защиты.

Фильтрация сигналов высокой частоты. схема встречного включения диодов в звонковую цепь или подводимую линию.

Литература к лекции [1, 2]

**Лекция 21.** Методы и средства защиты информации от устройств, использующих телефонную линию в качестве канала для передачи информации. (2 часа)

Метод линейного зашумления (низкочастотной маскирующей помехой). Метод высокочастотной широкополосной маскирующей помехи. Методы и средства защиты информации при ведении переговоров по телефонной линии. Метод синфазной низкочастотной маскирующей помехи Метод низкочастотной маскирующей помехи Метод низкочастотной маскирующей помехи Метод повышения напряжения Метод "обнуления".

Литература к лекции [1, 2, 3]

**Лекция 22.** Проектно-архитектурные мероприятия с целью защиты от утечки информации за счет ПЭМИН. (2 часа)

Основные правила оборудования помещений. радиоотражающие (экранирующие) и радиопоглощающие строительные и отделочные материалы (РЭМ и РПМ). Современные строительные технологии. Строительные конструкционные материалы Строительные тепло и звукоизоляционные материалы, для обеспечения поглощения с малым уровнем отражения электромагнитного поля. материалы с ячеистой структурой.

Литература к лекции [1]

**Лекция 23.** Средства защиты информации за счет ПЭМИН (2 часа)

Узлы и элементы электронной аппаратуры, в которых имеют место большие напряжения и протекают малые токи. Узлы и элементы электронной аппаратуры, в которых протекают большие токи и имеют место малые перепады напряжения. Электростатическое экранирование. Заземление электростатического экрана. Заземление электростатического экрана. Магнитостатическое экранирование. Эффективность магнитостатического экранирования.

Литература к лекции [2]

**Лекция 24.** Экранированные помещения и кабины (2 часа)

Классификация и эффективность экранирования помещений и кабин; локализация электромагнитного излучения; защита приемных устройств и специализированной аппаратуры; защита обслуживающего персонала от воздействия электромагнитного излучения. Выбор материала. Рекомендации по устройству и монтажу экранированных помещений

Литература к лекции [2, 4]

**Лекция 25.** Заземление. (2 часа)

Назначение, схемы и основные требования, предъявляемые к заземлению; одноточечные, многоточечные и комбинированные (гибридные) схемы. Зависимость величины сопротивления заземления от выбора заземлителя. Зависимость величины сопротивления заземления от сопротивления грунта; Развязывание информационных сигналов;

**Лекция 26.** Фильтрация (2 часа)

Электрический фильтр. Фильтры для цепей электропитания; фильтры для цепей управления и связи. Защита цепей питания. широкополосные LC-фильтры нижних частот; ферритовые помехоподавляющие изделия. Выбор типа фильтра. Практические рекомендации к применяемым фильтрам. Разделительные трансформаторы.

Литература к лекции [7, 8]

### 3.4. Лабораторные работы

№ п/п	Тема работы	Объем, час.
1	Организация аттестации выделенного помещения по требованиям безопасности информации.	2
2	Определение эффективности защищенности ПЭВМ	4
3	Исследование защиты речевой информации методом энергетического скрывтия	4
4	Определение и основные характеристики микрофонов	3
5	Исследование широкополосного приемника AR8600	4



<b>Итого по 5-му семестру</b>		<b>17</b>
6	Построение СКУД на базе биометрии. Штрих – коды.	2
7	Система охранного телевидения.	4
8	eToken.	4
9	Система охранной сигнализации.	3
10	iButton и интерком.	4
<b>Итого по 6-му семестру</b>		<b>17</b>
<b>Всего:</b>		<b>34</b>

### 3.5. Самостоятельная работа студента пятый семестр

№, п/п	Вид самостоятельной работы студента	Объем, час.
1	Проработка теоретического материала	9
2	Подготовка к лабораторным занятиям	10
3	Подготовка к экзамену и контрольные мероприятия	10
4	Индивидуальное задание	9
<b>Итого:</b>		<b>38</b>

### Самостоятельная работа студента шестой семестр

№, п/п	Вид самостоятельной работы студента	Объем, час.
1	Проработка теоретического материала	9
2	Подготовка к лабораторным занятиям	11
3	Подготовка к экзамену и контрольные мероприятия	10
4	Индивидуальное задание	9
<b>Итого:</b>		<b>39</b>

### 3.6. Индивидуальное задание

#### 3.6.1 Пятый семестр

Тематика индивидуального задания связана с проектированием и оформлением документации на объект информационной деятельности с целью закрепления навыков о комплексах и методах средств защиты информации, анализ существующих угроз, формирование модели нарушителя для адекватной защиты с учетом государственных и мировых стандартов в сфере информационной безопасности (согласно варианта задания).

#### 3.6.2 Шестой семестр

Тематика индивидуального задания связана с общей характеристикой задач моделирования КСЗИ. Сделать формальные модели безопасности и провести их анализ. Классификация формальных моделей безопасности. Изучить модели обеспечения конфиденциальности, модели обеспечения целостности. Субъектно-ориентированная модель. Прикладные модели защиты информации в АС. Формальное построение модели защиты: пример. Описание объекта защиты. Декомпозиция АС на субъекты и объекты. Модель безопасности: неформальное описание. Декомпозиция системы защиты информации. Противостояние угрозам. Реализация системы защиты информации субъекта АС субъектно-объектной модели. Формализация модели безопасности. Процедура создания пары субъект—объект, наделение их атрибутами безопасности. Осуществление доступа субъекта к объекту. Взаимодействие с внешними сетями. Удаление субъекта—объекта, анализ существующих угроз, формирование модели нарушителя для адекватной защиты с учетом государственных и мировых стандартов в сфере информационной безопасности (согласно варианта задания).

## 4. МЕТОДЫ КОНТРОЛЯ

В процессе изучения дисциплины «Методы и средства защиты информации» применяются следующие виды контроля:

1. Текущее тестирование или контрольный опрос по всем темам программы во время лекционных и лабораторных занятий
2. Оценка качества и своевременность выполнения СРС, относящейся к соответствующей теме. Учитывается качество и своевременность выполнения соответствующей лабораторной работы.
3. Промежуточная аттестация по результатам освоения дисциплины в семестре проводится в форме семестрового экзамена 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. в соответствии с графиком учебного процесса.

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

## 5. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

### Основная литература:

1. Мельников, В.П. Информационная безопасность и защита информации / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - М. : ИЦ "Академия", 2009. - 336с. - 2 экз
2. Грушо, А.А. Теоретические основы компьютерной безопасности / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М. : ИЦ "Академия", 2009. - 272с. - 18 экз
3. Мельников, В.П. Исследование систем управления / В. П. Мельников. - М. : ИЦ "Академия", 2008. - 336с. - 2 экз.
4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] / В. Ф. Шаньгин. - 74 Мб. - 2012. - 1 файл. - Систем. требования: Acrobat Reader.

### Дополнительная литература:

5. Андрианов В.И., Бородин В.А., Соколов А.В. Шпионские штучки “ и устройства для защиты объектов и информации: Справ. пособие. - С-Пб.: Лань, 1996. – 272 с.
6. Барсуков В.С., Марущенко В.В., Шигин В.А. Интегральная безопасность: Информационно-справочное пособие. - М.: РАО “Газпром”, 1994. – 170 с.

### Учебно-методические издания, разработанные в ДонНТУ

7. Методические указания к самостоятельной работе по дисциплине «Методы и средства защиты информации» - Донецк: ДонНТУ.
12. Методические указания к выполнению лабораторных работ по дисциплине «Методы и средства защиты информации» - Донецк: ДонНТУ.

### Периодические издания:

13. Автоматизация и современные технологии (2008-2013)
14. Бизнес и безопасность (2014)
15. Приборы и системы. Управление, контроль, диагностика (2007-2010)
16. Телекоммуникации (2007 - 2012)
17. Chip news инженерная микроэлектроника (2007 – 2012)

Составитель рабочей программы: \_\_\_\_\_

С.В. Константинов