

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



**УТВЕРЖДАЮ:**

Проректор по научно-педагогической работе

(подпись)

И.О. Фамилия

« 29 » 05

20 17 года

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**«Методы и средства 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	5	6	7
Общая трудоёмкость в з.е./часах	3,5/126	4,0/144	3,5/126
Аудиторные занятия (час.), в том числе	51	68	51
Лекции (час.)	34	34	34
Практические (семинарские) занятия (час.)	-	-	-
Лабораторные работы (час.)	17	34	17
Самостоятельная работа (час.), в том числе	39	40	75
Курсовой проект/работа (сем/кол.)	-	-	-
Индивидуальное задание (сем/кол.)	1	-	1
Форма промежуточной аттестации (экзамен/зачёт):	Экзамен	Экзамен	Зачет

Донецк, 2017 г.

Рабочая программа дисциплины «Методы и средства защиты информации» составлена в соответствии с учебным планом по направлению подготовки 10.03.01 – «Информационная безопасность» 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 « 13 » 09 20 16 года № 2

Заведующий кафедрой \_\_\_\_\_ (Паслён В.В.)

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

Протокол от « 15 » 09 20 16 года № 2

Заведующий кафедрой \_\_\_\_\_ (Паслён В.В.)

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

Протокол от « 13 » 09 20 16 года № 2

Председатель \_\_\_\_\_ (Паслён В.В.)

Рабочая программа **продлена** для 20 17 года приёма на заседании кафедры радиотехники и защиты информации:

Протокол от « 25 » 08 20 17 года № 10

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 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.)



## 1 ЦЕЛЬ И ЗАДАЧА УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью изучения дисциплины является формирование у студентов знаний и навыков 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 информационной деятельности 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 осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм (ОК-1); 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 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 определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ОПК-8); способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-3); способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-5); способность принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности (ПК-15); способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-19); способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК - 22).

## 2 МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина «Методы и средства защиты информации» относится к вариативной части дисциплин по выбору вуза профессионального цикла учебного плана; базируется на знаниях и умениях, которые студент приобрел при освоении предшествующих дисциплин: «Поля и волны в системах ТЗИ», «Физика», «Основы теории цепей, сигналов и процессов».

Знания и умения, приобретенные при освоении данной дисциплины, реализуются студентом при освоении последующих дисциплин обучения и прохождении производственной и преддипломной практик.

## 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. Термины и определения	6	4	-	2
Тема 2. Угрозы для информации. Объекты, подлежащие защите	6	4	-	2
Тема 3. Классификация и характеристика технических каналов утечки информации	9	4	4	1
Тема 4. Технические каналы утечки при передаче информации по каналам связи	10	4	4	2
Тема 5. Визуально оптические каналы утечки информации	10	4	4	2
Тема 6. Технические каналы утечки речевой информации	12	4	3	5
Тема 7. Средства ведения радио и радиотехнической разведки	10	4	-	6
Тема 8. Средства перехвата информации с проводных линий связи	8	2	2	4

Тема 9. Средства перехвата акустической информации.	5	2	-	3
Тема 10. Средства видеонаблюдения и съемки	5	2	-	3
<b>Итого по 5-му семестру:</b>	<b>81</b>	<b>34</b>	<b>17</b>	<b>30</b>
<b>6-й семестр</b>				
Тема 11. Классификация методов и средств защиты информации от утечки по техническим каналам	8	4	-	4
Тема 12. Звукоизоляция помещений	8	4	-	4
Тема 13. Акустическая и виброакустическая маскировка	14	4	6	4
Тема 14. Технические каналы утечки при передаче информации по каналам связи	16	4	8	4
Тема 15. Методы и средства обнаружения и подавления диктофонов и акустических закладок	16	4	8	4
Тема 16. Методы и средства защиты телефонных (слаботочных) линий	12	4	4	4
Тема 17. Средства защиты информации за счет ПЭМИН	8	4	-	4
Тема 18. Экранированные помещения и кабины	14	2	8	4
Тема 19. Заземление.	6	2	-	4
Тема 20. Фильтрация	6	2	-	4
<b>Итого по 6-му семестру:</b>	<b>108</b>	<b>34</b>	<b>34</b>	<b>40</b>
<b>7-й семестр</b>				
Тема 21. Создание комплекса технической защиты информации на объектах информационной деятельности.	14	4	-	10
Тема 22. Создание комплекса технической защиты информации. Предпроектные работы.	19	4	5	10
Тема 23. Порядок разработки и внедрения мероприятий по защите информации при создании комплекса технической защиты информации.	15	4	3	8
Тема 24 Назначение, структура и содержание управления КСЗИ	17	4	5	8
Тема 25 Сущность и содержание контроля функционирования Технологическое и организационное построение КСЗИ	10	4		6
Тема 26 Определение условий функционирования	12	6		8
Тема 27 Определение возможностей несанкционированного доступа к защищаемой информации	14	4	2	8
Тема 28. Создание комплексов технической защиты информации. Аттестация комплексов. Основные положения	16	6	2	8
<b>Итого по 7-му семестру:</b>	<b>117</b>	<b>34</b>	<b>17</b>	<b>66</b>
<b>Всего:</b>	<b>306</b>	<b>102</b>	<b>68</b>	<b>136</b>

### **3.2 Лекции**

#### **Лекция 1.** Введение.

(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.

Литература к лекции [1, 3]

#### **Лекция 2.** Термины и определения (2 часа)

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 [1,2, 6]

**Лекция 3.** 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 [3, 4]

#### **Лекция 4.** 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 5.** Утечка информации по техническим каналам. (2 часа)

Информации 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 6.** 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 подслушивания. Автономные средства разведки. Средства

инженерной защиты и технической охраны. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.

Литература к лекции [5,6]

**Лекция 7.** 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 8.** 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 [7,8]

**Лекция 9.** Основные положения современной концепции защиты информации техническими средствами (2 часа)

Основные направления инженерно-технической защиты информации. Задачи и принципы инженерно-технической защиты информации. Характеристика зонного принципа защиты информации.

Литература к лекции [6, 8]

**Лекция 10.** 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 [4, 5]

**Лекция 11.** Технические каналы утечки речевой информации (2 часа)

Воздушные: портативные диктофоны и проводочные микрофоны скрытого звукозаписи; направленные микрофоны; акустические радиозакладки, для передачи информации по радиоканалу; акустические сетевые закладки для передачи по линиям силовых сетей электропитания; виброакустические: электронные стетоскопы (вибродатчик с электронным усилителем) радиостетоскопы - для передачи информации по радиоканалу электронные стетоскопы с передачей информации в ИК диапазоне волн

Литература к лекции [8]

**Лекция 12.** Средства ведения радио и радиотехнической разведки (2 часа)  
Классификация. Организации радиоэлектронной разведки. История радиоэлектронной разведки в России. Сканирующие приемники

Литература к лекции [4, 5]

**Лекция 13.** Приборы контроля радиосвязи (радиотестеры) (2 часа)

Специальные приборы контроля радиосвязи (радиотестеры). состав приборов). Портативные ручные радиочастотомеры. Интерсепторы)

Литература к лекции [4,6]

**Лекция 14.** Аппаратно-программный комплекс информационно-технического воздействия в системах сотовой радиосвязи стандарта GSM 900/1800 (2 часа)

Назначение и основные функции. Состав комплекса. Радиопеленгаторы. Средства перехвата информации, обрабатываемой на ПК и ЭВМ. Системы разведки, предназначенные

для перехвата побочных электромагнитных излучений персональных компьютеров и ЭВМ. Основные характеристики систем.

Литература к лекции [2]

**Лекция 15.** 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 специализированных технических средствах. Методы и средства оценивания эффективности защиты акустической информации от утечки по виброакустическим каналам с использованием инструментальных средств.

Литература к лекции [2, 4, 5]

**Лекция 16.** Средства перехвата акустической информации. (2 часа)

(Проводные системы; Портативные диктофоны; Электронные стетоскопы; Акустически закладки; Направленные микрофоны; Лазерные акустические системы разведки.)

Литература к лекции [4,7]

**Лекция 17.** 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 18.** 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 19.** 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 20.** Звукоизоляция помещений. Звукоизоляция коммуникаций (2 часа)

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

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 [5, 6]

**Лекция 21.** Принципы оптической, радиоэлектронной, акустической разведок. (2 часа)

Средства наблюдения в оптическом диапазоне. Оптические системы. Визуально-оптические приборы. Фото и киноаппараты. Средства телевизионного наблюдения. Средства наблюдения в инфракрасном диапазоне. Средства наблюдения в радиодиапазоне

Литература к лекции [1, 2]

**Лекция 22.** 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 23.** 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, 5]

**Лекция 24.** Перехват информации, передаваемой по волоконно-оптическим линиям связи (2 часа)

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

Литература к лекции [1, 2]

**Лекция 25.** 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 [7]

**Лекция 26.** Методы и средства подавления диктофонов и акустических закладок (2 часа)

Частотные характеристики типичного фоновое 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 27.** 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, 8]

**Лекция 28.** 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 29.** 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, 5]

**Лекция 30.** 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, 6]

**Лекция 31.** 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, 8]

**Лекция 32.** Заземление. Фильтрация (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 33.** Фильтрация (2,6 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]

**Лекция 34.** Сущность и задачи комплексной защиты информации (2 часа)

Цели, задачи и принципы построения КСЗИ О понятиях безопасности и защищенности. Разумная достаточность и экономическая эффективность Управление безопасностью предприятия. Международные стандарты Цели и задачи защиты информации в автоматизированных системах. Современное понимание методологии защиты информации Особенности национального технического регулирования. Понятие безопасности ИТ. Документы пользователя. Требования к средствам обеспечения безопасности.

Литература к лекции [1, 4]

**Лекция 35.** Принципы организации и этапы разработки КСЗИ. (2 часа)

Методологические основы организации КСЗИ Разработка политики безопасности и регламента безопасности предприятия Основные положения теории сложных систем Система управления информационной безопасностью предприятия. Принципы построения и взаимодействие с другими подразделениями Требования, предъявляемые к КСЗИ. Требования к организационной и технической составляющим КСЗИ. Требования по безопасности, предъявляемые к изделиям ИТ. Этапы разработки КСЗИ

Литература к лекции [3,5]

**Лекция 36.** Факторы, влияющие на организацию КСЗИ (2 часа)

Влияние формы собственности на особенности защиты информации ограниченного доступа. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа. Характер основной деятельности предприятия. Состав, объекты и степень конфиденциальности защищаемой информации. Структура и территориальное расположение предприятия. Режим функционирования предприятия. Конструктивные особенности предприятия. Количественные и качественные показатели ресурсобеспечения. Степень автоматизации основных процедур обработки защищаемой информации.

Литература к лекции [2, 3, 4]

**Лекция 37.** Определение и нормативное закрепление состава защищаемой информации (2 часа)

Классификация информации по видам тайны и степеням конфиденциальности Нормативно-правовые аспекты определения состава защищаемой информации. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия. Методика определения состава защищаемой информации. Порядок внедрения Перечня сведений, составляющих КТ, внесение в него изменений и дополнений.

Литература к лекции [1, 2]

**Лекция 38.** Определение объектов защиты (2 часа)

Значение носителей защищаемой информации как объектов защиты. Методика выявления состава носителей защищаемой информации. Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации. Транспортные средства и особенности транспортировки. Состав средств обеспечения, подлежащих защите.

Литература к лекции [7,8]

**Лекция 39.** Дестабилизирующие воздействия на информацию и их нейтрализация (2 часа)

Факторы, создающие угрозу информационной безопасности. Угрозы безопасности информации. Модели нарушителей безопасности АС Подходы к оценке ущерба от нарушений ИБ. Обеспечение безопасности информации в непредвиденных ситуациях. Реагирование на инциденты. И Б. Резервирование информации и отказоустойчивость

Литература к лекции [5,6]

**Лекция 40.** Определение потенциальных каналов и методов несанкционированного доступа к информации (2 часа)

Технические каналы утечки информации, их классификация. Задачи КСЗИ по выявлению угроз и КУИ. Особенности защиты речевой информации. Особенности защиты компьютерной информации от утечки по каналам ПЭМИН

Литература к лекции [5]

**Лекция 41.** Определение возможностей несанкционированного доступа к защищаемой информации (2 часа)

Методы и способы защиты информации Классификация СЗИ НСД. Механизмы обеспечения безопасности информации. Идентификация и аутентификация. Разграничение доступа. Регистрация и аудит. Криптографическая подсистема. Межсетевое экранирование.

Методика выявления нарушителей, тактики их действий и состава интересующей их информации.

Литература к лекции [1, 2]

**Лекция 42.** Определение компонентов КСЗИ (2 часа)

Особенности синтеза СЗИ АС от НСД. Методика синтеза СЗИ. Общее описание архитектуры АС, системы защиты информации и политики безопасности. Формализация описания архитектуры, исследуемой АС. Формулирование требований к системе защиты информации. Выбор механизмов и средств защиты информации. Определение важности параметров средств защиты информации. Оптимальное построение системы защиты для АС. Выбор структуры СЗИ АС. Проектирование системы защиты информации для существующей АС

Литература к лекции [3, 5]

**Лекция 43.** Определение условий функционирования КСЗИ (2 часа)

Содержание концепции построения КСЗИ. Объекты защиты. Цели и задачи обеспечения безопасности информации. Основные угрозы безопасности информации АС организации. Основные положения технической политики в области обеспечения безопасности информации АС организации Основные принципы построения КСЗИ 10.8. Первоочередные мероприятия по обеспечению безопасности информации АС организации

Литература к лекции [4, 6]

**Лекция 44.** Разработка модели КСЗИ (2 часа)

Общая характеристика задач моделирования КСЗИ. Формальные модели безопасности и их анализ. Классификация формальных моделей безопасности 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.

Литература к лекции [5]

**Лекция 45.** Технологическое и организационное построение КСЗИ (2 часа)

Общее содержание работ по организации КСЗИ. Характеристика основных стадий создания КСЗИ. Назначение и структура технического задания (общие требования к содержанию). Предпроектное обследование, технический проект, рабочий проект. Аprobация и ввод в эксплуатацию.

Литература к лекции [5, 7]

**Лекция 46.** Кадровое обеспечение функционирования комплексной системы защиты информации (2 часа)

Специфика персонала предприятия как объекта защиты. Распределение функций по защите информации. Функции руководства предприятия. Функции службы защиты информации. Функции специальных комиссий. Обязанности пользователей защищаемой информации Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа. Подбор и обучение персонала.

Литература к лекции [7]

**Лекция 47.** Материально-техническое нормативно-методическое обеспечение комплексной системы защиты информации (2 часа)

Состав и значение материально-технического обеспечения функционирования КСЗИ. Перечень вопросов ЗИ, требующих документационного закрепления.

Литература к лекции [6, 7, 8]

**Лекция 48.** Назначение, структура и содержание управления КСЗИ (2 часа)

Понятие, сущность и цели управления КСЗИ. Принципы управления КСЗИ. Структура процессов управления. Основные процессы, функции и задачи управления КСЗИ. Основные стили управления. Структура и содержание общей технологии управления КСЗИ

Литература к лекции [1, 3, 4]

**Лекция 49.** Принципы и методы планирования функционирования КСЗИ (2 часа)

Понятие и задачи планирования функционирования КСЗИ Способы и стадии планирования Факторы, влияющие на выбор способов планирования. Основы подготовки и принятия решений при планировании Методы сбора, обработки и изучения информации, необходимой для планирования Организация выполнения планов.

Литература к лекции [1, 2]

**Лекция 50.** Сущность и содержание контроля функционирования. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций (2 часа)

Виды контроля функционирования КСЗИ. Цель проведения контрольных мероприятий в КСЗИ Анализ и использование результатов проведения контрольных мероприятий. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций. Технология принятия решений в условиях ЧС Факторы, влияющие на принятие решений в условиях ЧС. Подготовка мероприятий на случай возникновения ЧС

Литература к лекции [5]

**Лекция 51.** Общая характеристика подходов к оценке эффективности КСЗИ (2 часа)

Вероятностный подход Оценочный подход Требования РД СВТ и РДАС Задание требований безопасности информации и оценка соответствия им согласно ГОСТ 15408-2002. Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса. Экономический подход к оценке эффективности КСЗИ.

Литература к лекции [1, 4, 5]

### 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 скрывания	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.	8
7	Система охранного телевидения.	8
8	eToken.	8
9	Система охранной сигнализации.	6
10	iButton интерком.	4
<b>Итого по 6-му семестру</b>		<b>34</b>
11	Акт обследования. Порядок мероприятий	2
12	Акт категорирования	4
13	Статистический расчет угроз информации на КСЗИ	4
14	Подготовка технического задания.	3
15	Расчет экономической целесообразности КСЗИ	4



<b>Итого по 7-му семестру</b>	<b>17</b>
<b>Всего:</b>	<b>68</b>

### 3.5. Самостоятельная работа студента

№ п/п	Вид самостоятельной работы студента	Семестр		
		5-й	6-й	7-й
		Объем, час.		
1	Проработка теоретического материала	17	20	33
2	Подготовка к лабораторным занятиям	13	20	33
3	Выполнение индивидуальной работы	9	-	9
<b>Итого:</b>		<b>39</b>	<b>40</b>	<b>75</b>

### 3.6. Индивидуальное задание

#### 3.6.1 Индивидуальное задание 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 Индивидуальное задание седьмой семестр

Тематика индивидуального задания связана с общей характеристикой задач моделирования КСЗИ. Выполнить 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.
5. Кузнецов А.А. Защита деловой информации (секреты безопасности) / А. А. Кузнецов. - М. : Экзамен, 2008. - 255с. - 2 экз
6. Федоров Е.Е. Методы и средства обработки акустических сигналов / Е. Е. Федоров, В. А. Хорошко, Н. И. Чичикало. - ГВУЗ "ДонНТУ". - Донецк : Вебер, Донецк. отд-ние, 2009. - 424с. - 1 экз
7. Лавреш, И.И. Информационные технологии в региональном управлении [Электронный ресурс] / И. И. Лавреш, А. В. Трифонов. - ФГБОУ ВПО "Санкт-Петербург. гос. лесотехнический ун-т им. С.М. Кирова", Сыктывкар. лесной ин-т (филиал), Каф. инф-ц систем. - 1 Мб. - Сыктывкар : СЛИ, 2013. - 1 файл. - Систем. требования: Acrobat Reader

### **Дополнительная литература**

8. Методические рекомендации к самостоятельной работе студентов по дисциплине "Методы и средства защиты информации" = Методичні рекомендації до самостійної роботи студентів з навчальної дисципліни "Методи та засоби захисту інформації" [Электронный ресурс] : галузь знань: 1701 Інформаційна безпека : напрям підготовки: 6.170102 Системи технічного захисту інформації / Державний вищий навчальний заклад "Донецький національний технічний університет", Факультет радіотехніки та спеціальної підготовки ; ДВНЗ "ДонНТУ", Фак. радіотехніки і спец. підготовки, Каф. радіотехніки та захисту інформації ; уклад. І.Л. Щербов. - 15 Мб. - Донецьк : ДВНЗ "ДонНТУ", 2013. - 1 файл. - Систем. вимоги: Acrobat Reader.
9. Методические рекомендации к лабораторной работе студентов по дисциплине "Методы и средства защиты информации»

### **Периодические издания**

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

Составитель рабочей программы: \_\_\_\_\_ С.В. Константинов