МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ:
Проректор ДОННТУ
_____ А. Б. Бирюков
(подпись)
«08» 06 2021 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б12 Создание комплексных систем защиты информации

(наименование дисциплины согласно учебному плану)

Направление подготовки: 10.04.01 Информационная безопасность
(код и наименование направления / специальности)

Магистерская программа: Информационная безопасность
(наименование профиля / магистерской программы / специализации)

Программа: магистратура
(бакалавриат, магистратура, специалитет)

Форма обучения: очная
(очная, заочная, очно-заочная)

Форма обучения:	Очная
Семестр(ы)	**3-й**
Общая трудоёмкость в з.е./часах	**3 / 108**
Контактная работа (час.)	**55**
Лекции (час.)	17
Лабораторные работы (час.)	-
Практические (семинарские) занятия (час.)	34
Самостоятельная работа (час.), в том числе	**21**
Курсовой проект(работа) (семестр/час.)	-
Индивидуальное задание (кол./час.)	-
Контроль (экзамен, час./зачёт)	**Экзамен, 36**

Донецк, 2021 г.

Рабочая программа дисциплины «Создание комплексных систем защиты информации» составлена в соответствии с учебным планом по направлению подготовки 10.04.01 Информационная безопасность, магистерской программы «Информационная безопасность», очной формы обучения для 2021 года приёма.

Составитель:

проректор ГОУВПО «ДОННТУ» __________ (Щербов И. Л.)

ст. преп. каф. «Радиотехника и защита информации» __________ (Якушина А. Е.)

Рабочая программа **рассмотрена и утверждена** на заседании кафедры «Радиотехника и защита информации».

Протокол от «04» 06 2021 года № 12

Заведующий кафедрой ________________ (Паслен В.В.)
(подпись) (Ф.И.О.)

Рабочая программа **одобрена учебно-методической комиссией** ГОУВПО «ДОННТУ» по направлению подготовки 10.04.01 Информационная безопасность.

Протокол от «04» 06 2021 года № 4

Председатель ________________ (Паслен В.В.)
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры «Радиотехника и защита информации».

Протокол от «_____» ________________20___ года № ________

Заведующий кафедрой ________________ ____________________
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры «Радиотехника и защита информации».

Протокол от «_____» ________________20___ года № ________

Заведующий кафедрой ________________ ____________________
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры «Радиотехника и защита информации».

Протокол от «_____» ________________20___ года № ________

Заведующий кафедрой ________________ ____________________
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры «Радиотехника и защита информации».

Протокол от «_____» ________________20___ года № ________

Заведующий кафедрой ________________ ____________________
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры «Радиотехника и защита информации».

Протокол от «_____» ________________20___ года № ________

Заведующий кафедрой ________________ ____________________
(подпись) (Ф.И.О.)

1 ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью и задачами дисциплины «Создание комплексных систем защиты информации» являются: формирование у студентов знаний и умений по вопросам создания комплексных систем защиты информации в информационных системах различного назначения применяемых для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией.

В результате освоения учебной дисциплины студент должен:

– **знать** нормативные правовые акты и документы в сфере информационной безопасности; порядок отнесения сведений к информации с ограниченным доступом; требования к системе обеспечения информационной безопасности; методы и способы защиты информации в информационных системах; системы и средства защиты информации; состав и порядок построения комплексной системы защиты информации в информационных системах различного назначения; тенденции и перспективы развития средств проектирования системы информационной безопасности, а также смежных областей науки и техники; основные методики организации проектной деятельности;

– **уметь** разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности; разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности; осуществлять сбор, обработку и анализ информации, разрабатывать планы и программы проведения испытаний систем и средств защиты информации; использовать передовой отечественный и зарубежный опыт в профессиональной сфере деятельности; разрабатывать концепцию технического проекта по обеспечению информационной безопасности на всех этапах проблемы, формулируя цель, задачи, актуальность, значимость (научную, практическую, методическую), ожидаемые результаты;

– **владеть** навыками проектной деятельности по созданию технического задания системы защиты информации; технологиями и навыками организации и координации работы участников проекта по обеспечению информационной безопасности.

Перечисленные результаты обучения являются основой для формирования следующих компетенций выпускника:

– **ОПК-1.** Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

– **ОПК-2.** Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

2 МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина относится к обязательной части Блока 1 «Дисциплины (модули)» учебного плана. Базируется на знаниях, умениях и навыках, которые студент приобрел при освоении дисциплин бакалавриата (специалитета) по направлению подготовки в рамках укрупненной группы 10.00.00 Информационная безопасность.

Знания, умения и навыки, приобретенные при освоении данной дисциплины, реализуются студентом при прохождении производственных практик, государственной итоговой аттестации.

3 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Распределение учебных часов по темам дисциплины и видам занятий

№ темы	Наименование тем (содержательных модулей)	Количество часов				
		Всего	в том числе			
			лекции	практ.	лабор.	СРС
1	Законодательство в сфере информационной безопасности	2	1	0	0	1
2	Формирование общих требований к комплексной системе защиты информации в информационной системе	6	2	2	0	2
3	Разработка политики информационной безопасности в информационной системе	8	2	4	0	2
4	Разработка технического задания на создание комплексной системы защиты информации в информационной системе	22	4	12	0	6
5	Создание комплексной системы защиты информации в информационной системе, ввод в эксплуатацию	24	6	12	0	6
6	Аттестация комплексной системы защиты информации в информационной системе	10	2	4	0	4
Индивидуальное задание		0	0	0	0	0
Курсовая работа (проект)		0	0	0	0	0
Итого по видам занятий		72	17	34	0	21
Контроль		**36**				
Итого:		**108**				

Формирование компетенций в результате освоения тем дисциплины

Компетенции	Темы дисциплины, нацеленные на формирование компетенции
ОПК-1	Темы 1-6
ОПК-2	Темы 1-6

3.2 Лекции

Тема 1. Законодательство в сфере информационной безопасности

Содержание темы 1:

Законодательство в сфере информационной безопасности. Требования законодательных актов Донецкой Народной Республики в сфере информационной безопасности. Федеральная служба по техническому и экспортному контролю. Международные стандарты в сфере информационной безопасности.

Литература к теме 1: [1, 2, 4].

Тема 2. Формирование общих требований к комплексной системе защиты информации в информационной системе

Содержание темы 2:

Термины и определения. Исходные данные, обосновывающие необходимость создания комплексной системы защиты информации в информационной системе. Обследование информационной системы. Последовательность выполнения и типовое содержание работ каждого из этапов создания комплексной системы защиты информации.

Литература к теме 2: [1, 2, 4].

Тема 3. Разработка политики информационной безопасности в информационной системе

Содержание темы 3:

Подбор базовых решений по противодействию всем существенным угрозам, формирование общих требований, правил, ограничений, рекомендаций и т.д., которые регулируют использование защищенных технологий обработки информации в информационной системе. Определение меры и средств защиты информации. Документальное оформление политики информационной безопасности.

Литература к теме 3: [1, 2, 4].

Тема 4. Разработка технического задания на создание комплексной системы защиты информации в информационной системе

Содержание темы 4:

Определение требований к защите информации. Определение технических систем и средств защиты информации. Определение этапов создания порядок создания комплексной системы защиты информации. Порядок проведения всех видов испытаний и ввода в эксплуатацию.

Литература к теме 4: [1, 2, 4].

Тема 5. Создание комплексной системы защиты информации в информационной системе, ввод в эксплуатацию

Содержание темы 5:

Порядок разработки проекта. Эскизный проект. Технический проект. Рабочий проект. Эксплуатационная документация. Подготовка комплексной системы защиты информации к вводу в эксплуатацию. Специальные исследования и инструментальные измерения.

Литература к теме 5: [1, 2, 4].

Тема 6. Аттестация комплексной системы защиты информации в информационной системе

Содержание темы 6:

Порядок проведения опытной эксплуатации. Оценка полноты и качества работ. Аттестация комплексной системы защиты информации в информационной системе.

Литература к теме 6: [1, 2, 4].

3.3 Практические занятия

№ п/п	Тема работы	Объем, час.	Литература
1	Формирование общих требований к комплексной системе защиты информации в информационной системе	2	[3]
2	Разработка политики информационной безопасности в информационной системе	4	[3]
3	Разработка технического задания на создание комплексной системы защиты информации в информационной системе	12	[3]
4	Создание комплексной системы защиты информации в информационной системе, ввод в эксплуатацию	12	[3]
5	Аттестация комплексной системы защиты информации в информационной системе	4	[3]
Итого:		**34**	

3.4 Лабораторные работы

В учебном плане не запланировано.

3.5 Самостоятельная работа студента

№, п/п	Вид самостоятельной работы студента	Объем, час.
1	Изучение лекционного материала	7
2	Подготовка к практическим занятиям	14
Итого:		**21**

3.6 Индивидуальное задание и курсовой проект (работа)

Индивидуальное задание и курсовой проект (работа) учебным планом не предусмотрены.

4 ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1 Критерии и шкалы для интегрированной оценки уровня сформированности компетенций

Составляющая компетенции – полнота знаний

– нулевой уровень: неверные, не аргументированные, с множеством грубых ошибок ответы на вопросы. Уровень знаний ниже минимальных требований;

– минимальный уровень: даны не полные, неточные и неаргументированные ответы на вопросы. Допущено много грубых ошибок. Уровень знаний ниже минимальных требований;

– пороговый уровень: даны недостаточно полные, точные и аргументированные ответы на вопросы. Плохо знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено много негрубых ошибок;

– средний уровень: даны достаточно полные, точные и аргументированные ответы на вопросы. В целом знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько негрубых ошибок;

– продвинутый уровень: даны полные, точные и аргументированные ответы на вопросы. Знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько негрубых ошибок;

– высокий уровень: даны полные, точные и аргументированные ответы на вопросы. Знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько неточностей.

Составляющая компетенции – умения

– нулевой уровень: полное отсутствие понимания сути методики решения задачи, допущено множество грубейших ошибок / задания не выполнены вообще;

– минимальный уровень: слабое понимание сути методики решения задачи, допущены грубые ошибки. Решения не обоснованы. Не умеет использовать нормативно-техническую литературу;

– пороговый уровень: достаточное понимание сути методики решения задачи, допущены ошибки. Решения не всегда обоснованы. Умеет использовать нормативно-техническую литературу. Слабо ориентируется в специальной научной литературе;

– средний уровень: в целом понимает суть методики решения задачи, допущены ошибки. Решения не всегда обоснованы. Умеет использовать нормативно-техническую и специальную научную литературу;

– продвинутый уровень: в целом понимает суть методики решения задачи, допущены неточности. Способен обосновать решения. Умеет использовать нормативно-техническую и специальную научную литературу;

– высокий уровень: понимает суть методики решения задачи. Способен обосновать решения. Умеет использовать нормативно-техническую и специальную научную литературу, передовой производственный опыт.

Составляющая компетенции – владение навыками

– нулевой уровень: не демонстрирует владение навыками выполнения профессиональных задач. Не может выполнить задания;

– минимальный уровень: не демонстрирует владение навыками выполнения профессиональных задач. Испытывает существенные трудности при выполнении отдельных заданий;

– пороговый уровень: владеет навыками выполнения профессиональных задач на пороговом уровне. Задания выполняет медленно и некачественно;

– средний уровень: владеет навыками выполнения профессиональных задач. Задания выполняет на среднем уровне по быстроте и качеству;

– продвинутый уровень: владеет уверенными навыками выполнения профессиональных задач. Быстро и качественно выполняет задания, иногда допуская незначительные погрешности;

– высокий уровень: владеет уверенными навыками выполнения профессиональных задач. Быстро и качественно выполняет задания, при необходимости демонстрируя творческий подход.

Обобщенная оценка сформированности компетенций

– нулевой уровень: на нулевом уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;

– минимальный уровень: на минимальном уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;

– пороговый уровень: на пороговом уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;

– средний уровень: на среднем уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;

– продвинутый уровень: на продвинутом уровне сформированы: все составляющие; одна или две из трёх, остальные – на высоком уровне;

– высокий уровень: на высоком уровне сформированы все составляющие компетенций.

4.2 Вопросы к экзамену и пример экзаменационного билета

Вопросы к экзамену:

1. Какие сведения не могут быть отнесены к государственной тайне?
2. Какие сведения относятся к государственной тайне?
3. Какие сведения подлежат защите в государственных информационных системах?
4. Какие свойства информации подлежат защите в информационных системах?
5. Что означает термин «Носители сведений, составляющих государственную тайну»?
6. Что означает термин «Техническая защита секретной информации»?
7. Что означает термин «Техническое средство в защищенном исполнении»?
8. Что означает термин «Средства защиты информации»?
9. Что означает термин «Угроза для секретной информации»?
10. Что означает термин «Утечка секретной информации»?
11. Законодательство в сфере информационной безопасности. Требования законодательных актов Донецкой Народной Республики в сфере информационной безопасности.
12. Федеральная служба по техническому и экспортному контролю. Международные стандарты в сфере информационной безопасности.
13. В каких случаях создается комплексная система защиты информации в информационных системах?
14. Что понимается под защитой информации от несанкционированного доступа?
15. Что понимается под защитой информации от утечки по техническим каналам за счет побочных электромагнитных излучений?
16. Что понимается под защитой информации от утечки по техническим каналам за счет побочных электромагнитных наводок?
17. Что понимается под силовым воздействием на информационную систему?
18. Этапы создания комплексной системы защиты информации в информационных системах.
19. Порядок обследования информационной системы. Информация и технология её обработки.
20. Порядок обследования информационной системы. Физическая среда.
21. Порядок обследования информационной системы. Вычислительная система.
22. Порядок обследования информационной системы. Персонал.
23. Формирование задачи по созданию комплексной системы защиты информации.
24. Разработка политики информационной безопасности в информационной системе.
25. Служба защиты информации. Структура, цели, задачи.
26. Модель угроз.
27. Модель нарушителя.
28. Принятие решения на защиту информации. Оценка риска.

29. Техническое задание на создание комплексной системы защиты информации. Назначение, состав, порядок утверждения.

30. Состав комплекса технической защиты информации от утечки по техническим каналам за счет побочных электромагнитных излучений.

31. Состав комплекса технической защиты информации от утечки по техническим каналам за счет побочных электромагнитных наводок.

32. Состав комплекса технической защиты информации от утечки по техническим каналам за счет электроакустических преобразований.

33. Состав комплекса технической защиты информации от утечки по акустическим и виброакустическим техническим каналам.

34. Состав комплекса технической защиты информации от специальных воздействий.

35. Состав комплекса технической защиты информации от утечки за счет несанкционированного доступа.

36. Оценка эффективности защиты информации. Проведение исследований от утечки по акустическому и виброакустическому каналам.

37. Оценка эффективности защиты информации. Проведение исследований от утечки по техническим каналам за счет побочных электромагнитных наводок.

38. Оценка эффективности защиты информации. Проведение исследований от утечки по техническим каналам за счет электроакустических преобразований.

39. Аттестация комплексной системы защиты информации в информационных системах.

Пример экзаменационного билета:

ГОУВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Уровень высшего профессионального образования: **Магистратура**

Направление подготовки: **10.04.01 Информационная безопасность**

Профиль: **Информационная безопасность**

Семестр: **3-й семестр**

Учебная дисциплина: **«Создание комплексных систем защиты информации»**

БИЛЕТ № 01

1. Какие сведения подлежат защите в государственных информационных системах?
2. Что понимается под защитой информации от утечки по техническим каналам за счет побочных электромагнитных наводок?
3. Формирование задачи по созданию комплексной системы защиты информации.
4. Состав комплекса технической защиты информации от утечки по техническим каналам за счет побочных электромагнитных излучений.
5. Оценка эффективности защиты информации. Проведение исследований от утечки по акустическому и виброакустическому каналам.

Утверждено на заседании кафедры «Радиотехника и защиты информации».

Протокол № __ от _____

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

Экзаменатор _____ (Щербов И. Л.)
(подпись) (Ф.И.О.)

КРИТЕРИИ

оценивания экзаменационной работы

по дисциплине «Создание комплексных систем защиты информации»

для обучающихся по направлению подготовки 10.04.01. Информационная безопасность

Экзамен проводится письменно по билетам. Билет содержит 5 вопросов, каждый из которых требует конкретного ответа. При необходимости отвечающий должен подготовить проект документа, в соответствии с требованиями нормативных актов.

Вопросы охватывают теоретическую часть курса, а также требуют демонстрации практических навыков, полученных студентом в ходе практических занятий.

Правильный ответ на 1 вопрос оценивается в пять баллов, на 2-4 вопрос оценивается в десять баллов, на 5 вопрос оценивается в пятнадцать баллов. Если ответ не полный, то он оценивается соответственно в два, пять и восемь баллов. При отсутствии правильного ответа на поставленный вопрос обучающийся получает ноль баллов.

Полученные баллы за ответы на вопросы билета суммируются.

С учётом результатов текущего контроля работы студента выводится итоговая оценка по 100-балльной шкале.

Полученная оценка по 100-балльной шкале определяет оценку по государственной шкале и шкале ESTS.

Утверждено на заседании кафедры радиотехники и защиты информации,
протокол № ___ от __.___.20___ г.
Заведующий кафедрой _____ Паслен В.В.

4.3 Критерии оценивания

Оценивание уровня освоения студентом учебного материала дисциплины «Создание комплексных систем защиты информации» производится в ходе текущего контроля и промежуточной аттестации (семестрового контроля).

Текущий контроль знаний студента осуществляется по результатам выполнения практических занятий. Выполнение заданий на практических занятиях, является необходимым условием допуска студента к прохождению промежуточной аттестации

Текущий контроль знаний студента осуществляется по результатам практических занятий. Распределение баллов текущего контроля работы студента на протяжении семестра приведено в таблице.

Распределение баллов текущего контроля

Форма контроля	Количество баллов	Примечание
Отчёт о выполнении задания на практическом занятии	10	Задание выполнено правильно, студент глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, не затрудняется с ответом при видоизменении заданий, использует в ответе материал дополнительной литературы, осуществляет анализ и делает выводы
	8	Задание выполнено в целом правильно, студент достаточно полно владеет учебным материалом, обоснованно его излагает, но при освещении некоторых вопросов не хватает достаточной глубины и аргументации, допускаются при этом отдельные несущественные неточности и незначительные ошибки
	6	Задание выполнено в целом правильно, студент владеет значительной частью учебного материала, освещает его основное содержание, неспособен к глубокому, всестороннему анализу, обоснованию и аргументации, допускает существенные неточности и ошибки.
Итого по практическим занятиям	**50**	Всего: 10*5 практических.
ИТОГО:	**50**	Максимально возможное

Промежуточная аттестация по результатам освоения дисциплины в семестре проводится в форме семестрового экзамена.

Форма проведения семестрового экзамена – письменная. Экзаменационный билет включает в себя 5 теоретических вопросов.

При оценивании студента на экзамене преподаватель руководствуется критериями, приведенными в таблице 2.

Максимальное количество баллов за ответ на вопрос экзаменационного билета засчитывается студенту в случае, если ответ подтверждает владение студентом знаниями в полном объеме учебной программы, материал изложен в логической последовательности с выделением главного, содержит точные формулировки, сопровождается иллюстрирующими схемами и рисунками (при необходимости).

Правильный ответ на 1 вопрос оценивается в пять баллов, на 2-4 вопрос оценивается в десять баллов, на 5 вопрос оценивается в пятнадцать баллов. Если ответ не полный, то он оценивается соответственно в два, пять и восемь баллов. При отсутствии правильного ответа на поставленный вопрос обучающийся получает ноль баллов.

Распределение баллов по семестровому экзамену

Форма контроля		Максимально возможное количество баллов
Ответ на вопросы экзаменационного билета	вопрос 1	5
	вопрос 2	10
	вопрос 3	10
	вопрос 4	10
	вопрос 5	15
ИТОГО		**50**

Итоговая оценка определяется путем суммирования количества баллов по результатам текущего контроля и количества баллов по результатам семестрового экзамена. Максимально возможное количество баллов – 100.

Полученная оценка по 100-балльной шкале определяет оценку по государственной шкале и шкале ESTS:

Сумма баллов по 100-бальной шкале	Оценка по шкале ECTS	Оценка по государственной шкале
90-100	A	Отлично
80-89	B	Хорошо
75-79	C	
70-74	D	Удовлетворительно
60-69	E	
35-59	FX	Неудовлетворительно
0-34	F*	

* – с обязательным повторным изучением дисциплины.

4.4 Пример текущего опроса на практических занятиях

На примере темы «Создание комплексной системы защиты информации в информационной системе, ввод в эксплуатацию»:

1. Этапы создания комплексной системы защиты информации в информационных системах.

2. Порядок обследования информационной системы. Информация и технология её обработки.

3. Порядок обследования информационной системы. Физическая среда.

4. Порядок обследования информационной системы. Вычислительная система.

5. Порядок обследования информационной системы. Персонал.

Ответы на вопросы входного контроля учитываются преподавателем в результатах текущего контроля работы студента.

4.5 Курсовое проектирование

Учебным планом курсовое проектирование не запланировано.

5 РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

I. Основная литература

1. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. – Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. – 267 с. – ISBN 978-5-9515-0426-5. – Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. – URL: https://www.iprbookshop.ru/101929.html. – Режим доступа: для авторизир. пользователей

2. Методы и средства комплексной защиты информации в технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. – Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. – 224 с. – ISBN 978-5-9515-0429-6. – Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. – URL: https://www.iprbookshop.ru/101925.html. — Режим доступа: для авторизир. пользователей

II. Дополнительная литература

3. Ворожейкин, В. Н. Технические средства и методы защиты информации – дополнительные главы : лабораторный практикум / В. Н. Ворожейкин. – 2-е изд. – Самара : Самарский государственный технический университет, ЭБС АСВ, 2019. – 336 с. – Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. – URL: https://www.iprbookshop.ru/111432.html. – Режим доступа: для авторизир. пользователей

4. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – 2-е изд. – Саратов : Профобразование, 2019. – 702 с. – ISBN 978-5-4488-0070-2. – Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. – URL: https://www.iprbookshop.ru/87995.html. – Режим доступа: для авторизир. пользователей.

6 УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5. Методические указания к выполнению практических и контрольных работ, внеаудиторной самостоятельной работы по дисциплине «Создание комплексных систем защиты информации» : для студентов направления подготовки 10.04.01 Информационная безопасность / ГОУВПО «ДОННТУ», Каф. радиотехники и защиты информации ; сост.: И. Л. Щербов, А. Е. Якушина. – Донецк : ДОННТУ, 2017. – Текст : электронный // Электронный каталог Научно-технической библиотеки Донецкого национального технического университета. – Доступ через личный кабинет студента.

Электронно-информационные ресурсы

ЭБС ДОННТУ – http://donntu.org/library

ЭБС «IPRbooks» – http://www.iprbookshop.ru

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Лекционные и практические занятия

Учебная аудитория 7.506 учебный корпус 7, для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специализированная мебель: доска аудиторная, парты, столы. Оборудование: ПК – Intel Celeron 1,7 GHz, Asus P4S8X-X, 512 Mb DDR, 40 Gb IDE, SIS S3 Savage 4, Windows XP SP3, монитор Samtron 78DFS; мультимедийный проектор, экран. Специализированное ПО: Libreoffice 5.3.4 (лицензия GNU GPL).

Лаборатория «Специальных исследований и специальных проверок» 7.530 учебный корпус 7, для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специализированная мебель: доска аудиторная, парты, столы. Оборудование: ПК: Intel Pentium Dual-core CPU E5300 2,6 GHz, Gigabyte GA-G41M-Combo, 2048 Mb DDR II, 1 Tb IDE, ATI Radeon HD 5670, Windows XP SP3, монитор LG FLATRON E1951C-BN; антенна 1.20 Супрал, макет 11-ти элементной ДМВ-антенны, макет 11-ти элементной МВ-антенны, макет 19-ти элементной ДМВ-антенны, макет 3-х элементной FM-антенны, макет 5-ти элементной TV-антенны, макет GSM-антенны (параболическая R=0,2 м), макет GSM-антенны (прямоугольная L=1,5м), макет GSM-антенны (прямоугольная L=1,8м), макет спутниковой антенны, установка для изучения волн явлений на поверхности воды ФПВ, установка для изучения звуковых волн ФПВ-03. Специализированное ПО: MATLAB и Simulink 2015a (Student Version), LabView 8.2 (base license), Libreoffice 5.3.4 (лицензия GNU GPL), ANSYS 19.1 (Student version), MMANA GAL V. 3.0.0.3 (Basic), CST STUDIO SUITE (Student Edition), HyperWorks 14.0 (Student Edition).

7.2 Самостоятельная работа

Помещения для самостоятельной работы с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации: читальные залы, учебные корпуса 2, 3 (Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду (ЭИОС ДОННТУ) и электронно-библиотечную систему (ЭБС IPRbooks), а также возможностью индивидуального неограниченного доступа обучающихся в ЭБС и ЭИОС посредством Wi-Fi с персональных мобильных устройств. ОС – Microsoft Windows 7, OpenOffice 2.0.3 – общественная лицензия MPL 2.0 / Grub loader for ALT Linux – лицензия GNU LGPL v3/ Mozilla Firefox – лиц. MPL2.0, Moodle (Modular Object-Oriented Dynamic Learning Environment) – лиц. GNU GPL.