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

УТВЕРЖДАЮ:
Первый проректор
_____ А.А. Каракозов
(подпись)
«_31_» ___03___ 20_23_ года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.10 Обеспечение информационной безопасности в инфокоммуникациях
(код и наименование дисциплины согласно учебному плану)

Направление подготовки: 11.04.04 Электроника и наноэлектроника
(код и наименование направления подготовки / специальности)

Направленность (профиль): Промышленная электроника
(наименование профиля / магистерской программы /специализации)

Программа: магистратура
(бакалавриат, магистратура, специалитет)

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

Форма обучения	очная	заочная
Семестр	3	3
Общая трудоёмкость в з.е./часах	3.5/126	3.5/126
Контактная работа (час.), в том числе:	72	20
лекции (час.)	34	8
лабораторные работы (час.)	34	6
практические (семинарские) занятия (час.)	0	0
Самостоятельная работа (час.), в том числе:	18	70
курсовой проект/работа (семестр)	0	0
Контроль (экзамен, час./зачёт)	экзамен, 36	экзамен, 36

Донецк, 2023 г.

Рабочая программа дисциплины «Обеспечение информационной безопасности в инфокоммуникациях» составлена в соответствии с учебным планом по направлению подготовки 11.04.04 «Электроника и наноэлектроника» (профиль подготовки «Промышленная электроника») для 2023 года приёма по очной и заочной формам обучения.

Составитель:
заведующий кафедрой автоматики
и телекоммуникаций, к.т.н., профессор _____ Турупалов В.В.
(подпись)

Рабочая программа **рассмотрена и принята** на заседании кафедры автоматики и телекоммуникаций.

Протокол от «8» марта 2023 года № 3

Заведующий кафедрой _____ Турупалов В.В.
(подпись)

Рабочая программа **рассмотрена и принята** на заседании кафедры электронной техники.

Протокол от «17» марта 2023 года № 8.

Заведующий кафедрой _____ Кузнецов Д.Н.
(подпись)

Рабочая программа **одобрена учебно-методической комиссией** ГОУВПО «ДОННТУ» по направлению 11.04.04 - Электроника и наноэлектроника.

Протокол от «17» марта 2023 года № 3.

Председатель _____ Кузнецов Д.Н.
(подпись)

Рабочая программа **согласована с выпускающей кафедрой** электронная техника.

Заведующий кафедрой _____ Кузнецов Д.Н.
(подпись)

Рабочая программа **одобрена учебно-методической комиссией** ГОУВПО «ДОННТУ» по направлению подготовки 11.04.04 «Электроника и наноэлектроника».

Протокол от «__» _____ 20__ года № __

Председатель _____ Кузнецов Д.Н.
(подпись)

1. ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на рассмотрение основных проблем защиты телекоммуникационных сетей, классификации и характеристик угроз безопасности, принципов управления риском и критериев оценки безопасности, принципов криптографической защиты.

Целью преподавания дисциплины является формирование у магистрантов представлений о главных требованиях по защите информации, организационно-технических мероприятиях по обеспечению безопасности в системах телекоммуникаций, основных аспектах безопасности мобильных радиосредств связи, обеспечивающих качественную подготовку магистров по направлению подготовки 11.04.04 «Электроника и наноэлектроника» (профиль подготовки «Промышленная электроника»)).

В результате освоения дисциплины магистрант должен

знать: тенденции и перспективы развития защиты информации; типовые угрозы информационной безопасности; критерии оценки безопасности по национальным и международным стандартам; структуру комплексной системы защиты безопасности; главные требования по защите информации; методы и средства несанкционированного доступа к телекоммуникационным системам.

уметь: использовать системный подход к анализу угроз безопасности; пользоваться техническими и криптографическими методами защиты средств связи; применять комплекс организационно-технических мероприятий по обеспечению безопасности в системах телекоммуникаций; классифицировать угроз информационной безопасности;

владеть: навыками шифрования и дешифрования информации; навыками выбора мер обеспечения информационной безопасности; навыками оценки угроз информационной безопасности.

Перечисленные результаты обучения являются основой для формирования следующих компетенций:

– способностью осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1);

– способностью приобретать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению инженерных задач (ОПК-3);

– способностью разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решения инженерных задач (ОПК-4);

– готовностью формулировать цели и задачи научных исследований в

соответствии с тенденциями и перспективами развития электроники и наноэлектроники, а также смежных областей науки и техники, способностью обоснованно выбирать теоретические и экспериментальные методы и средства решения сформулированных задач (ПК-1);

– способностью проектировать устройства, приборы и системы электронной техники с учетом заданных требований (ПК-5).

2. МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина относится к обязательной части Блока 1 дисциплин (модулей) учебного плана.

Базируется на знаниях и умениях, которые обучающийся приобрел при освоении предшествующих дисциплин, освоенных программой бакалавриата по соответствующему направлению.

Знания и умения, приобретенные при освоении данной дисциплины, реализуются студентом при изучении последующей дисциплины «Проектирование микропроцессорных систем», «Проектирование электронных средств и систем», «Математические модели информационных систем», «Проектирование микропроцессорных систем», прохождении учебной практики: научно-исследовательской работы (получение первичных навыков научно-исследовательской работы), производственной практики: научно-исследовательской работы, прохождении государственной итоговой аттестации.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Распределение учебных часов по темам дисциплины и видам занятий

№ темы	Наименование темы (содержательных модулей)	Количество часов (очная / заочная форма)				
		Всего	В том числе			
			Лекции	Практ. (Семин.)	Лабор.	СР
1	Введение	3	2/0	0	0	1/3
2	Проблемы защиты телекоммуникационных сетей	8	2/1	0	4/1	2/6
3	Классификация методов и средств обеспечения безопасности в каналах телекоммуникаций	9	2/1	0	5/1	2/7
4	Классификация и характеристика угроз безопасности	10	4/1	0	4/1	2/8
5	Принципы управления риском и критерии оценки безопасности	8	2/1	0	4/0	2/7
6	Организационно-технические мероприятия по обеспечению безопасности в системах телекоммуникаций	11	4/1	0	5/1	2/9
7	Методы и средства несанкционированного доступа к телекоммуникационным системам	12/10	6/1	0	4/1	2/8
8	Технические методы и средства защиты проводных средств связи	8	6/1	0	0	2/7
9	Аспекты безопасности мобильных радиосредств связи	10	4/1	0	4/1	2/8
10	Криптографическая защита	7	2/0	0	4/0	1/7
Контактная работа (дополнительная)		4/6				
Курсовой проект		0				
Итого по видам занятий		86/84	34/8	0	34/6	18/70
Контроль		36				
ИТОГО		**126**				

Формирование компетенций в результате освоения тем дисциплины

Компетенции	Темы дисциплины, нацеленные на выработку компетенции
УК-1	Темы 2, 5, 6
ОПК-3	Темы 1-10
ОПК-4	Темы 1-10
ПК-1	Темы 2, 3, 4
ПК-5	Темы 2, 3,4, 5, 6, 7, 8, 9, 10

3.2 Лекции

Тема 1. Введение

Содержание темы 1:

Задание и структура курса. Обзор содержания лекций, лабораторных работ. Основная и дополнительная литература. Актуальность проблем обеспечения информационной безопасности.

Литература к теме 1: [1,2,5]

Тема 2. Проблемы защиты телекоммуникационных сетей

Содержание темы 2:

Защита телекоммуникационных сетей. Защита информации в телекоммуникационных сетях. Трудности защиты информации в сетях связи. Главные требования по защите информации.

Литература к теме 2: [2,5,6]

Тема 3. Классификация методов и средств обеспечения безопасности в каналах телекоммуникаций

Содержание темы 3:

Методы защиты. Средства защиты. Комплекс средств защиты. Политика безопасности.

Литература к теме 3: [3,4,6]

Тема 4. Классификация и характеристика угроз безопасности

Содержание темы 4:

Угрозы информационной безопасности. Базовые признаки информационной безопасности. Способы предотвращения и обнаружения угроз. Частота, последствия и защита от угроз.

Литература к теме 4: [1,2,4]

Тема 5. Принципы управления риском и критерии оценки безопасности

Содержание темы 6:

Определение степени риска. Выбор мер обеспечения безопасности. Сертификация и утверждение. Планирование нештатных ситуаций. Принципы управления риском.

Литература к теме 6: [3,5,6]

Тема 6. Организационно-технические мероприятия по обеспечению безопасности в системах телекоммуникаций

Содержание темы 6:

Организационные меры. Технические меры. Криптографические меры.

Литература к теме 5: [1,4,6]

Тема 7. Методы и средства несанкционированного доступа к телекоммуникационным системам

Содержание темы 7:

Перехват радиопереговоров. Системы прослушивания сообщений, передаваемых по сотовым каналам. Снятие информации с проводных средств связи. Снятие информации с волоконнооптических линий связи.

Литература к теме 7: [2,4,5]

Тема 8. Технические методы и средства защиты проводных средств связи

Содержание темы 8:

Защита телефонных аппаратов и линий связи. Профессиональные средства защиты информации.

Литература к теме 8: [1,2,4,6]

Тема 9. Аспекты безопасности мобильных радиосредств связи

Содержание темы 9:

Общее описание характеристик безопасности. Безопасность в стандарте GSM. Системы защиты от фрода

Литература к теме 9: [1,3,5]

Тема 10. Криптографическая защита

Содержание темы 10:

Принципы криптографичекой защиты. Применение шифрования в средствах связи. Криптографические методы и средства защиты.

Литература к теме 10: [4,5]

3.3 Практические (семинарские) занятия

В учебном плане не запланировано.

3.4 Лабораторные работы

№ п/п	Тема занятия	Объем, час. (очн/заочн)	Литература
1	Шифры Полибия, Тритемия, Цезаря	4/1	[8]
2	Шифры Виженера	5/1	[8]
3	Шифры Кардано и Ардженти	4/1	[8]
4	Шифры с вариацией размера окна шифрования и Вернама	4/0	[8]
5	Сеть Фейстеля	5/1	[8]
6	Алгоритм RSA	4/1	[8]
7	Парольная защита	4/1	[8]
8	Частотный анализ	4/0	[8]
ИТОГО:		**34/6**	

3.5 Самостоятельная работа студента

№ п/п	Виды самостоятельной работы студента	Объем, час. (очн/заочн)
1	Изучение лекционного материала	10/40
2	Подготовка к практическим занятиям	0
3	Подготовка к лабораторным занятиям	8/30
4	Выполнение курсового проекта	0
5	Выполнение курсовой работы	0
ИТОГО:		**18/70**

3.6 Курсовой проект (работа), индивидуальное задание

Учебным планом заочной формы обучения в рамках освоения дисциплины предусмотрено выполнение студентами контрольной работы по форме **индивидуального задания.**

Тематика задания связана с изучением методов решений систем сравнений. Цель – усвоение принципов проведения инженерных расчетов для последующего применения в криптографии.

В результате выполнения работы студент должен:

– знать принципы целочисленного деления;

– знать основы терминологии, применяемой при сравнении чисел;

– уметь решать системы сравнений первой степени с помощью китайской теоремы об остатках;

– уметь использовать функцию Эйлера для решения систем сравнений.

Задание на контрольную работу выбирается обучающимися заочной формы в соответствии с методическими указаниями [9, 10], согласовывается с преподавателем и выполняется по методическими рекомендациям [9, 10].

Отчет о работе состоит из текстовой части на листах формата А4. Ввыполнение индивидуального задания осуществляется с применением специального программного обеспечения для научных и инженерных расчетов. Рекомендуемый объем пояснительной записки по индивидуальному заданию – не более 12 страниц формата А4 (210×297 мм).

4 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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. Актуальность проблем обеспечения информационной безопасности.
2. Безопасность мобильных радиосредств связи. Безопасность в стандарте GSM. Механизмы аутентификации.
3. Проблемы защиты телекоммуникационных сетей.
4. Безопасность мобильных радиосредств связи. Общее описание характеристик безопасности
5. Главные требования по защите информации. Доступность. Целостность и точность. Конфиденциальность.
6. Безопасность в стандарте GSM. Общий состав секретной информации и ее распределение в аппаратных средствах.
7. Классификация методов и средств обеспечения безопасности в каналах телекоммуникаций.
8. Безопасность в стандарте GSM. Обеспечение секретности в процессе корректировки местоположения. Процедура корректировки местоположения
9. Классификация угроз безопасности. По природе возникновения. По степени преднамеренности проявления.
10. Безопасность в стандарте GSM. Установка режима шифрования. Обеспечение секретности абонента.
11. Характеристика угроз безопасности. Аппаратные сбои. Вирусы.
12. Безопасность мобильных радиосредств связи. Общее описание характеристик безопасности.
13. Принципы управления риском и критерии оценки безопасности.
14. Безопасность мобильных радиосредств связи. Безопасность в стандарте GSM. Механизмы аутентификации.
15. Организационные мероприятия по обеспечению безопасности в системах телекоммуникаций.
16. Безопасность в стандарте GSM. Ключ шифрования.
17. Технические меры по обеспечению безопасности в системах телекоммуникаций.
18. Безопасность в стандарте GSM. Установка режима шифрования. Обеспечение секретности абонента.
19. Методы и средства несанкционированного доступа к телекоммуникационным системам. Перехват радиопереговоров.
20. Безопасность в стандарте GSM. Обеспечение секретности в процессе корректировки местоположения. Процедура корректировки местоположения.

21. Снятие информации с проводных средств связи. Непосредственное подключение к телефонной линии.
22. Безопасность в стандарте GSM. Общий состав секретной информации и ее распределение в аппаратных средствах.
23. Снятие информации с проводных средств связи. Индукционное подсоединение к телефонной линии.
24. Методы и средства несанкционированного доступа к телекоммуникационным системам. Снятие информации с проводных средств связи. Радиопередающее подключение к телефонной линии, телефонные радиоретрансляторы.
25. Снятие информации с проводных средств связи. Слушанье через звонковую цепь.
26. Снятие информации с проводных средств связи. Внутрикомнатное прослушивание с применением высокочастотной накачки.
27. Методы и средства несанкционированного доступа к телекоммуникационным системам. Снятие информации с волоконнооптических линий связи.

ГОУВПО «Донецкий национальный технический университет»

Уровень высшего профессионального образования: магистратура

Направление подготовки (специальность): 11.04.02 "Инфокоммуникационные технологии и системы связи"

Профиль (магистерская программа, специализация): «Инфокоммуникационные технологии и системы связи»

Семестр: осенний

Учебная дисциплина: Обеспечение безопасности в информационных системах

БИЛЕТ №1

1. Характеристика угроз безопасности. Аппаратные сбои. Вирусы.
2. Зашифровать трехраундовой сетью Фейстеля.

№	ключи			открытый текст							
21	4	1	3	1	1	0	0	0	0	1	0

3. Безопасность в стандарте GSM. Ключ шифрования.
4. Алгоритм RSA. Найти закрытый ключ и расшифровать сообщение.

p	q	e	C
13	29	211	147

Утверждено на заседании кафедры Автоматики и телекоммуникаций

(наименование кафедры полностью)

Протокол № __ от ___

Зав. кафедрой _____ Турупалов В.В.

(подпись) (Ф.И.О.)

Экзаменатор _____ Турупалов В.В.

(подпись) (Ф.И.О.)

КРИТЕРИИ
оценивания экзаменационной работы
по дисциплине «Обеспечение безопасности в информационных системах»
для обучающихся по направлению подготовки
11.04.02 «Инфокоммуникационные технологии и системы связи»
(магистерская программа – Инфокоммуникационные технологии и системы связи)

Экзамен проводится письменно по билетам. Билет содержит 2 теоретических вопроса и 2 практических задания. При необходимости отвечающий должен сопроводить написанное поясняющим рисунком.

Теоретические вопросы охватывают теоретическую часть курса, практические задания требуют демонстрации практических навыков, полученных студентом в ходе выполнения лабораторных работ.

Правильный ответ на теоретический вопрос оценивается в пятнадцать баллов. Если ответ не полный, то он оценивается в восемь баллов. При отсутствии правильного ответа на поставленный вопрос обучающийся получает ноль баллов. Полученные баллы за ответы на вопросы билета суммируются и 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 автоматики и телекоммуникаций,
протокол № ___ от __.___.20___ г.
Заведующий кафедрой _____ Турупалов В.В.

4.3 Критерии оценивания

Оценивание уровня освоения студентом учебного материала дисциплины «Обеспечение безопасности в информационных сетях» производится в ходе текущего контроля и промежуточной аттестации (семестрового контроля).

Текущий контроль знаний студента очной формы обучения осуществляется по результатам лабораторных работ; студента заочной формы обучения – по результатам выполнения контрольной работы (индивидуального задания).

Выполнение лабораторных работ с защитой отчёта, выполнение индивидуального задания (контрольной работы), предусмотренных рабочей программой дисциплины, является необходимым условием допуска студента к экзамену. Распределение баллов текущего контроля работы студента на протяжении семестра приведено в таблице 1.

Таблица 1 – Распределение баллов текущего контроля

Форма контроля	Возможное количество баллов	Примечание
Для студентов очной формы обучения		
Отчёт по лабораторной работе	5	Задание выполнено правильно, решения обоснованы, приведен анализ полученного результата
	3	Задание выполнено в целом правильно, решения не всегда обоснованы, возникли трудности в объяснении полученных результатов
Итого по	**40**	Из расчёта проведения четырех

Форма контроля	Возможное количество баллов	Примечание
лабораторным работам (максимально возможное)		лабораторных работ. Оценивается каждая работа.
ИТОГО:	**40**	Максимально возможное
Для студентов заочной формы обучения		
Выполнение контрольной работы (индивидуального задания)	**40**	При выполнении задания приняты правильные решения, изложение материала аргументированное, последовательное, работа оформлена без замечаний
	20	Задание выполнено в целом правильно, но решения не всегда обоснованы, имеются замечания по оформлению.
ИТОГО:	**40**	Максимально возможное

Промежуточная аттестация по результатам освоения дисциплины в семестре проводится в форме семестрового экзамена. Форма проведения экзамена – письменная. Экзаменационный билет включает в себя 2 теоретических вопроса и 2 практических задания. 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).

Таблица 2 – Распределение баллов по семестровому экзамену

Форма контроля		Максимально возможное количество баллов
Ответ на вопросы экзаменационного билета	вопрос 1	15
	вопрос 2	15
	вопрос 3	15
	вопрос 4	15
ИТОГО:		**60**

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 ECTS:

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

Сумма баллов по 100-бальной шкале	Оценка по шкале ECTS	Оценка по государственной шкале
60-69	E	
35-59	FX	Неудовлетворительно
0-34	F*	

* – с обязательным повторным изучением дисциплины.

4.4 Пример текущего опроса на лабораторных работах

На примере темы «Классификация и характеристика угроз безопасности»:

1. Понятие угрозы информационной безопасности.
2. Классификация угроз информационной безопасности по природе возникновения.
3. Классификация угроз информационной безопасности по степени преднамеренности проявления.
4. Классификация угроз информационной безопасности по непосредственному источнику угроз.
5. Классификация угроз информационной безопасности по положения источника угроз.
6. Классификация угроз информационной безопасности по степени воздействия на защищаемую систему.

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

4.5 Курсовое проектирование

В учебном плане не запланировано.

5. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

I Основная литература

1. Гатченко, Н.А. Криптографическая защита информации [Электронный ресурс] : учебное пособие для вузов / Н. А. Гатченко, А. С. Исаев, А. Д. Яковлев ; Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев ; Санкт-Петербург. нац. исслед. ун-т информ. технологий, механики и оптики. - 2 Мб. - Санкт-Петербург : НИУ ИТМО, 2012. - 1 файл. - Систем. требования: Acrobat Reader. – Режим доступа http://ed.donntu.org/books/17/cd6859.pdf. - Загл. с экрана.

2. Басалова, Г.В. Основы криптографии [Электронный ресурс] : [курс лекций] / Г. В. Басалова ; Г.В. Басалова. - 66 Мб. - М. : ИНТУИТ, 2016. - 1 файл. - Систем. требования: Acrobat Reader. – Режим доступа http://ed.donntu.org/books/cd4856.pdf. - Загл. с экрана.

3. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А. А. Бирюков ; А.А. Бирюков. - 10 Мб. - Москва : ДМК Пресс, 2012. - 1 файл. - Систем. требования: Acrobat Reader. – Режим доступа http://ed.donntu.org/books/20/cd10154.pdf. - Загл. с экрана.

4. Романьков В.А. Алгебраическая криптография [Электронный ресурс] : монография / В. А. Романьков ; В.А. Романьков ; ФГБОУ ВПО "Омск. гос. ун-т им.

М.Ф. Достоевского. - 843 Кб. - Омск : Изд-во ОмГТУ, 2013. - 1 файл. - Систем. требования: Acrobat Reader.

II Дополнительная литература

5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие для студентов технических вузов / В. Ф. Шаньгин ; В.Ф. Шаньгин ; гл. ред. Д.А. Мовчан. - 74 Мб. - Москва : ДМК Пресс, 2012. - 1 файл. - Систем. требования: Acrobat Reader. – Режим доступа http://ed.donntu.org/books/17/cd7025.pdf. - Загл. с экрана.

6. Мэйволд, Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд ; Э. Мэйволд ; Нац. Открытый Ун-т "ИНТУИТ". - 2-е изд., испр. - 58 Мб. - Москва : ИНТУИТ, 2016. - 1 файл. - Систем. требования: Acrobat Reader. – Режим доступа http://ed.donntu.org/books/17/cd6857.djvu. - Загл. с экрана.

7. Яковлев, В.А. Шпионские и антишпионские штучки [Электронный ресурс] / В. А. Яковлев ; В.А. Яковлев. - 25 Мб. - Санкт-Петербург : Наука и техника, 2015. - 1 файл. - Систем. требования: Просмотрщик djvu-файлов. – Режим доступа http://ed.donntu.org/books/cd4854.pdf. - Загл. с экрана.

6 УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебно-методические издания, разработанные в ДонНТУ:

8. Методические указания к выполнению лабораторных работ по дисциплине «Обеспечение безопасности в информационных сетях»: для магистрантов направления подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи» (магистерская программа «Инфокоммуникационные технологии и системы связи») всех форм обучения / ГОУВПО “ДОННТУ”, Каф. автоматики и телекоммуникаций ; сост.: В. В. Турупалов, А. В. Дзюба. – Донецк : ДОННТУ, 2020. – Систем. требования: Acrobat Reader. – Загл. с титул. экрана.

9. Методические указания к выполнению индивидуального задания по дисциплине «Обеспечение безопасности в информационных сетях» : для магистрантов направления подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи» (магистерская программа «Инфокоммуникационные технологии и системы связи») всех форм обучения / ГОУВПО “ДОННТУ”, Каф. автоматики и телекоммуникаций ; сост.: В. В. Турупалов, А.В. Дзюба. – Донецк : ДОННТУ, 2020. – Систем. требования: Acrobat Reader. – Загл. с титул. Экрана.

10. Методические указания для самостоятельной работы студентов по дисциплине «Обеспечение безопасности в информационных сетях» : для магистрантов направления подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи» (магистерская программа «Инфокоммуникационные технологии и системы связи») всех форм обучения / ГОУВПО “ДОННТУ”, Каф. автоматики и телекоммуникаций ; сост.: В. В. Турупалов, А. В. Дзюба. – Донецк : ДОННТУ, 2020. – Систем. требования: Acrobat Reader. – Загл. с титул. экрана.

Электронно-информационные ресурсы

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

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Учебная аудитория № 8.607, учебный корпус 8, для проведения лекционных и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (мультимедийное оборудование: персональный компьютер с выходом в сеть и возможностью подключения к сети «Интернет» (P IV-1.7 GHz); экран проекционный ELIT SCREENS M113XWS1; коммутационный шкаф; Swich TP-Link; patchpanel; wi-fi точка доступа.

Специализированная мебель: столы; магнитно-маркерная доска. Системное обеспечение: операционная система Windows XP Professional x86/64 (академическая лицензия DreamSparkPremium); OpenOffice 2.0.3 (общественная лицензия MPL 2.0); Google Slides (бесплатная версия); Mozilla Firefox (общественная лицензия MPL 2.0)).

2. Учебная аудитория № 8.608, учебный корпус 8, для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (мультимедийное оборудование: персональные компьютеры с выходом в сеть (iC DualCore 1.6 Ghz; iPE2140-1.6Ghz; iC DualCore 1.6 Ghz); экран проекционный Sopar 180*180. Лабораторное оборудование: генератор ГЗ-102; генератор Г6-28; частотомер электронносчетный Ч3-33; источник питания пост. тока Б5-46; осциллограф универсальный С1-79; стойка приборная ДК 7067; микроскоп МБС-9; мультиметр В 1025; анализатор спектра HP 8753C; анализатор спектра HP 8569B; многофункциональный синтезатор HP 8904A; частотомер HP 5372A; генератор сигналов HP8656B4; стабилизатор ТЭС-15; генератор Г6-28; частотомер универсальный цифровой Ч334; измеритель индукционный емкостной высокочастотный Е12-1; прибор для исследования АЧХ Х1-50; стабилизированный выпрямитель ТВ-1; микролаб КР580ИК80. Специализированная мебель: столы; магнитно-маркерная доска. Системное обеспечение: операционная система Windows XP Professional x86/64 (академическая лицензия DreamSparkPremium); OpenOffice 2.0.3 (общественная лицензия MPL 2.0); Google Slides (бесплатная версия); Mozilla Firefox (общественная лицензия MPL 2.0); GNU Octave-6.1.0 (общественная лицензия)).

3. 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, 8 (аудитория №8.001) (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. Системное обеспечение: операционная система Microsoft

Windows 7 (академическая лицензия, OpenOffice 2.0.3 (общественная лицензия MPL 2.0), Mozilla Firefox (общественная лицензия MPL 2.0), Moodle (Modular Object-Oriented Dynamic Learning Environment) (общественная лицензия GNU).