

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



УТВЕРЖДАЮ:

Проректор по научно-педагогической работе

«29» 05 20 17 года

А.В. Левин

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность информационных и коммуникационных систем»

(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
Общая трудоёмкость в з.е./часах	3,0/108	2,5/90
Аудиторные занятия (час.), в том числе	51	51
Лекции (час.)	34	34
Практические (семинарские) занятия (час.)	-	-
Лабораторные работы (час.)	17	17
Самостоятельная работа (час.), в том числе	39	39
Курсовой проект/работа (сем/кол.)	-	-
Индивидуальное задание (сем/кол.)	1	1
Форма промежуточной аттестации (экзамен/зачёт):	Экзамен	Зачет

Донецк, 2017 г.

Рабочая программа дисциплины «Безопасность информационных
и коммуникационных систем»

составлена в соответствии с учебным планом по направлению подготовки 10.03.01 – «Информационная безопасность» для 20 17 года приёма.

Составитель: А.В. Оводенко

Оводенко А.В., доцент, ~~старший преподаватель~~ кафедры радиотехники и защиты информации

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

Протокол от « » 20 года №

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

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

Протокол от « » 20 года №

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

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

Протокол от «13» 09 20 16 года № 2

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

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

Протокол от «25» 05 20 17 года № 10

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

Согласовано с выпускающей кафедрой радиотехники и защиты информации.

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

Согласовано с выпускающей кафедрой радиотехники и защиты информации.

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

Согласовано с выпускающей кафедрой радиотехники и защиты информации.

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

1. ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины - приобретение студентами теоретических и практических навыков в области обеспечения безопасности информации, связанных с конфиденциальностью, целостностью, аутентификацией, а также знакомство с практическим использованием профессиональных средств информационных технологий в профессиональной деятельности. В соответствии с требованием образовательного стандарта в дисциплине изучаются фундаментальные понятия об информации, методах ее получения, хранения, обработки, передачи и программировании, а также роли информационного ресурса и информационной культуры в информатизации общества.

В результате освоения дисциплины студент должен:

- знать: базовые понятия информатики, информационные системы и технологии, сетей и телекоммуникаций, баз данных; виды угроз и нарушений в информационных системах, их причины; методы обеспечения информационной безопасности на предприятиях; понятие государственной, коммерческой и личной тайны; применять инструментальные средства получения, хранения, переработки информации.

- уметь: прогнозировать тенденции информационного развития общества, оценивать социальную значимость выбранной профессии; выявлять и анализировать угрозы информационной безопасности; обосновывать правовые, организационные, инженерно-технические, программно-аппаратные меры по защите информации; использовать современные стандарты и методики; общий состав и структуру персональных компьютеров и вычислительных систем.

1. Требования к уровню освоения содержания дисциплины

В процессе освоения дисциплины формируются следующие компетенции: ОК-1, ПК-3, ПК-8, ПК-9, ПК-14, ПК-18.

2. Содержание дисциплины (основные разделы)

Технологии Ethernet. Беспроводные локальные сети стандарта 802.11. Технологии физического уровня стандарта 802.11. Безопасность беспроводных LAN. Исследование протоколов механизмов защиты информации в компьютерных системах и сетях. Обнаружение нарушения безопасности в сетях. Анализ трафика. Фильтры для контроля сетевого трафика. Технология взлома.

2. МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина относится к циклу дисциплин профессиональной и практической подготовки нормативной части учебного плана.

Дисциплина базируется на знаниях и умениях, обеспечивающих базовую теоретическую и инженерную подготовку. Фундаментальной основой для изучения дисциплины являются знания полученные на дисциплинах «Высшая математика», «Теория вероятности», «Основы дискретной математики».

Знания и умения, приобретенные при освоении данной дисциплины, реализуются студентом при выполнении курсовых работ (проектов) по всем дисципли-

нам профессиональной и практической подготовки и дипломном проектировании.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Распределение учебных часов по темам дисциплины и видам занятий

Наименование тем (содержательных модулей)	Количество часов				
	Всего	В том числе			
		Лекции	Практ. (Семина.)	Лабор.	СРС
Тема 1. Понятие информационной безопасности.	21	3	2	6	10
Тема 2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.	18	5	1	4	8
Тема 3. Виды угроз информационной безопасности Российской Федерации	23	6	1	6	10
Тема 4. Источники угроз информационной безопасности Российской Федерации.	16	5	2	2	7
Тема 5. Информационная безопасность и информационное противодействие.	18	6	2	3	7
Тема 6. Поточные шифры	18	6	2	2	8
Тема 7. Источники ключей	20	8	2	2	8
Тема 8. Модель систем аутентификации	21	7	3	2	9
Тема 9. Методы обеспечения целостности и подлинности	22	4	3	4	11
Тема 10. Цифровая подпись	21	3	2	5	11
Тема 11. Анализ электронной цифровой подписи	22	3	3	5	11
Тема 12. Цифровые подписи в группе точек эллиптических кривых	24	5	3	5	11
Тема 13. Оценка подлинности защиты информации	26	7	3	5	11
Итого:	270	68		51	

3.2. Лекции

Тема 1 Понятие информационной безопасности. Национальная безопасность. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутривнутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства (4 ауд / 3 сам).

Тема 2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере. (6 ауд/3 сам).

Тема 3. Виды угроз информационной безопасности Российской Федерации. Угрозы конституцион-

ным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.

Угрозы информационному обеспечению государственной политики Российской Федерации.

Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходе этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Угрозы безопасности информационных систем, как уже развернутых, так и создаваемых на территории России. (4 ауд / 3 сам).

Тема 4. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности. (4 ауд / 3 сам).

Тема 5. Информационная безопасность и информационное противоборство. Субъекты информационного противоборства.

Тема 6. Основные направления обеспечения информационной безопасности объектов информационной сферы государства. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. (6 ауд / 4 сам).

Тема 7. Общие методы обеспечения информационной безопасности Российской Федерации. Правовые, организационные и технические методы обеспечения информационной безопасности РФ. (6 ауд / 4 сам).

Тема 8. Методы и средства обеспечения безопасности компьютерных систем. Компьютерная система как объект информационной безопасности. Общая характеристика методов и средств защиты информации. Технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности КС. (15 ауд / 6 сам).

Тема 9. Итоги изучения дисциплины за 9 семестр (2 ауд / 0 сам).

Тема 10. Комплексная защита информации - сущность и задачи (1 час).

Предмет, задачи и структура КЗИ. Роль и место КЗИ в формировании специалиста. Рекомендации по изучению материала. Обзор литературы.

Тема 11. Стратегии комплексной защиты информации, стадии их создания (1 час).

Определение стратегии КЗИ. Виды стратегии: оборонительная, наступательная, упреждающая.

Тема 12. Структура, характеристики принципы построения и папы разработки комплексной защиты информации объекта (1 час).

Определение структуры КЗИ. Основные характеристики КЗИ. Этапы построения КЗИ по видам стратегий. Жизненный цикл построения КЗИ.

3.3. Практические (семинарские) занятия

По данному предмету не предусмотрены.

3.4. Лабораторные работы

№ п/п	Тема работы	Объем, час.	Литература
1	Шифр замены.	10	[1]
2	Шифр перестановки	5	[2]
3	Гамирование	5	[2]
4	Стандарт шифрования данных DES.	5	[3]

5	Стандарт криптографического преобразования данных ГОСТ 28147-89.	5	[4]
6	Криптографическая система RSA	5	[5]
7	Распределение ключей. Протокол Диффи-Хеллмана.	5	[5]
8	Эллиптические кривые в криптографии.	2	[5]
9	Генерирование случайных чисел.	2	[10]
10	Шифр эль-Гамала.	8	[11]
11	Цифровая подпись.	6	[12]
Итого:		51	

3.5. Самостоятельная работа студента

№ п/п	Виды самостоятельной работы студента	Объем, час.
1	Изучение лекционного материала (не менее 50% от объема лекций)	34
2	Подготовка к практическим занятиям (не менее 50% от объема аудиторных практических занятий)	34
3	Подготовка к лабораторным работам (не менее 50% от объема аудиторных лабораторных занятий)	40
Итого:		108

3.6. Курсовой проект (работа), индивидуальное задание

Курсовой проект (работа) по дисциплине учебным планом не предусмотрен.

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Текущий контроль знаний студентов производится по результатам выполнения лабораторных работ, индивидуального задания, во время контрольных опросов в ходе проведения практических занятий.

Промежуточная аттестация по результатам освоения дисциплины в семестре проводится в форме семестрового экзамена в соответствии с «Положением об организации и проведении семестрового контроля знаний студентов в Донецком национальном техническом университете», утвержденном 25.09.2013 года.

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

5. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Основные источники:

1. Башлы, П.Н. Информационная безопасность / П.Н. Башлы. – Ростов н/Д: Феникс, 2009. – 253 с.

2. Галатенко, В.А. Основы информационной безопасности. Курс лекций. Учебное пособие. / В.А. Галатенко. – М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2011. – 264 с.

3. Галатенко, В.А. Стандарты информационной безопасности. / В.А. Галатенко. – М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2008. – 264 с.

Составитель рабочей программы: В.А. Галатенко В.А. Ф.И.О.
(подпись)