

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



УТВЕРЖДАЮ:

Проректор по научно-педагогической работе

А.В. Левин
(подпись) И.О. Фамилия

« 29 » 05 20 17 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптография и стеганография»

(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	4,0/144	3,5/126
Аудиторные занятия (час.), в том числе	68	51
Лекции (час.)	34	34
Практические (семинарские) занятия (час.)	-	-
Лабораторные работы (час.)	34	17
Самостоятельная работа (час.), в том числе	40	21
Курсовой проект/работа (сем/кол.)	-	-
Индивидуальное задание (сем/кол.)	-	-
Форма промежуточной аттестации (экзамен/зачёт):	Экзамен	Экзамен

Донецк, 2017 г.

Рабочая программа дисциплины «Криптография и стеганография» составлена в соответствии с учебным планом по направлению подготовки 10.03.01 – «Информационная безопасность» для 2017 года приёма.

Составитель: 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 « 15 » 09 2016 года № 2

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

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

Протокол от « 25 » 05 2016 года № 10

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

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

Протокол от « 25 » 05 2016 года № 10

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

Рабочая программа **продлена** для 2017 года приёма на заседании кафедры радиотехники и защиты информации.

Протокол от « 25 » 05 2017 года № 10

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

Согласовано с выпускающей кафедрой радиотехники и защиты информации.

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

Рабочая программа **продлена** для 2018 года приёма на заседании кафедры радиотехники и защиты информации.

Протокол от « 31 » 08 2018 года № 1

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

Согласовано с выпускающей кафедрой радиотехники и защиты информации.

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

Рабочая программа **продлена** для 2019 года приёма на заседании кафедры радиотехники и защиты информации.

Протокол от « 28 » 08 2019 года № 1

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

Согласовано с выпускающей кафедрой радиотехники и защиты информации.

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

1 ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина рассматривает вопросы информационной безопасности, связанные с сокрытием информации в информационно-телекоммуникационных системах.

Целью изучения дисциплины «Криптография и стеганография» является приобретение студентами теоретических и практических навыков в области обеспечения безопасности информации, связанных с конфиденциальностью, целостностью, аутентификацией и невозможностью отказа сторон от авторства.

В результате освоения дисциплины студент должен:

Знать основные задачи, решаемые криптографией и методы их решения; основные понятия, применяемые в современной криптографии; способы шифрования; алгоритмы основных систем шифрования; достоинства и недостатки основных методов; основные блочные и поточные системы шифрования; системы шифрования с открытыми ключами и симметричные криптосистемы; протоколы идентификации; криптографические хэш-функции; цифровые подписи; протоколы распределения ключей и возможные атаки на них; основные национальные нормативные документы в области защиты информации с помощью криптографических методов.

Уметь классифицировать шифры по различным признакам; решать основные задачи на применение криптографических алгоритмов; применять в профессиональной деятельности современный математический аппарат; ориентироваться в методологии и подходах к применению различных криптографических систем, ограничениях и способах их применения.

Перечисленные результаты обучения являются основой для формирования следующих компетенций: способность осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-6); способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления (ОК-7); способность логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-8); способность к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства (ОК-10); 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 использовать нормативные правовые документы в своей профессиональной деятельности (ОПК-3); 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 принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-1); способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-3); способность использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-8); способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности (ПК-9); способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов (ПК-14); способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-18); способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-19).

2 МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина относится к циклу дисциплин профессиональной подготовки базовой части учебного плана и 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 дисциплинам 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	лабор.	СРС
5-й семестр					
Тема 1. Вычислительно стойкие и вероятно устойчивые криптосистемы	14	2	-	6	6
Тема 2. Математические модели криптопреобразования	18	6	-	6	6
Тема 3. Криптопреобразования в группах точек эллиптических кривых	16	6	-	6	6
Тема 4. Асимметрично направленное шифрование класса RSA	13	4	-	4	5
Тема 5. Симметричные криптопреобразования	18	6	-	6	6
Тема 6. Поточные шифры	16	6	-	4	6
Тема 7. Источники ключей	11	4	-	2	5
Итого по 5-му семестру	108	34	-	34	40
6-й семестр					
Тема 7. Источники ключей	12	4	-	2	2
Тема 8. Модель систем аутентификации	21	6	-	2	4
Тема 9. Методы обеспечения целостности и подлинности	22	4	-	4	4
Тема 10. Цифровая подпись	21	4	-	-	1
Тема 11. Анализ электронной цифровой подписи	22	4	-	4	3
Тема 12. Стеганография	24	4	-	4	3
Тема 13. Проблемы синтеза сетей засекреченной связи	26	8	-	1	4
Итого по 6-му семестру	72	34	-	17	21
ВСЕГО	180	68	-	51	61

3.2. Лекции

Тема 1. Вычислительно стойкие и вероятно устойчивые криптосистемы

Содержание темы 1:

Тема 1.1. Условия осуществления криптоанализа.

Тема 1.2. Определение вычислительно-стойкой криптосистемы и условия реализации.

Тема 1.3. Определение вероятно устойчивой криптосистемы

Литература к теме 1: [1]

Тема 2. Математические модели криптопреобразования.

Содержание темы 2:

Тема 2.1. Классификация криптопреобразования.

Тема 2.2. Математические модели асимметричного криптопреобразования.

Литература к теме 2: [1]

Тема 3. Криптопреобразования в группах точек эллиптических кривых.

Содержание темы 3:

Тема 3.1. Метрика (арифметика над эллиптическими кривыми).

Тема 3.2. Базисы представления.

Тема 3.3. Общие параметры и ключи.

Литература к теме 3: [1]

Тема 4. Асимметрично направленное шифрование класса RSA.

Содержание темы 4:

Тема 4.1. Алгоритм направленного шифрования.

Тема 4.2. Синтез ключей.

Тема 4.3. Оценка криптостойкости.

Литература к теме 4: [2,3]

Тема 5. Симметричные криптопреобразования

Содержание темы 5:

Тема 5.1. Классификация симметричных криптопреобразований.

Тема 5.2. Основы криптопреобразования симметричного типа.

Тема 5.3. Понятие блочного шифра.

Литература к теме 5: [3]

Тема 6. Поточные шифры.

Содержание темы 6:

Тема 6.1. Математическая модель

Тема 6.2. Шифры Вернама и смирения.

Тема 6.3. Примеры реализации.

Литература к теме 6: [1, 5,12]

Тема 7. Источники ключей.

Содержание темы 7:

Тема 7.1. Требования к генераторам ключей.

Тема 7.2. Основные алгоритмы генерации ключей.

Тема 7.3. Оценка свойств.

Тема 7.4. Методы и средства генерирования и распределения ключей.

Литература к теме 7: [6]

Тема 8. Модель систем аутентификации.

Содержание темы 8:

Тема 8.1. Общие понятия модели угроз.

Тема 8.2. Введение в теорию аутентификации (теория Сименсона).

Литература к теме 8: [7]

Тема 9. Методы обеспечения целостности и подлинности

Содержание темы 9:

Тема 9.1. Методы аутентификации в симметрично и асимметричных криптосистемах.

Тема 9.2. Методы имитозащиты с использованием имитоприкладок.

Тема 9.3. Парадокс «День рождения».

Литература к теме 9: [9, 10,11]

Тема 10. Цифровая подпись.

Содержание темы 10:

Тема 10.1. Основные понятия.

Тема 10.2. Классификация и методы осуществления ЭЦП.

Тема 10.3. Электронная цифровая подпись в кольце.

Литература к теме 10: [12]

Тема 11. Анализ электронной цифровой подписи

Содержание темы 11:

Тема 11.1. Проблемные вопросы устойчивости ЭЦП в кольцах и полях RSA

Тема 11.2. Особенности применения электронной цифровой подписи.

Литература к теме 11: [5, 11]

Тема 12. Стеганография

Содержание темы 12:

Тема 12.1. Общие сведения. Классическая стеганография

Тема 12.2. Компьютерная стеганография.

Литература к теме 12: [5, 11]

Тема 13. Проблемы синтеза сетей засекреченной связи

Содержание темы 13:

Тема 13.1. Сети шифрованной связи. Организация сетей конфиденциальной связи. Основные термины и понятия. Угрозы сетям. Протоколы распределения ключей и их характеристики.

Тема 13.2. Компрометация абонентов сети; способы построения протоколов распределения ключей, обеспечивающих защиту от компрометации. Способы восстановления шифрованной связи после компрометации. Подходы к локализации негативных последствий компрометации. Проблемы синхронизации в сетях шифрованной связи и методы их решения.

Тема 13.3. Подходы к снижению вероятности повторного использования. Современные тенденции развития средств и методов криптографической защиты информации. Программно-аппаратная реализация современных криптографических средств.

Литература к теме 13: [5, 11]

3.4. Лабораторные работы

№ п/п	Тема работы	Объем, час.	Литература
1	Шифр замены.	6	[1]
2	Шифр перестановки	6	[2]
3	Гамирование	6	[2]
4	Стандарт шифрования данных DES.	6	[3]
5	Стандарт криптографического преобразования данных ГОСТ 28147-89.	4	[4]
6	Криптографическая система RSA	4	[5]
7	Распределение ключей. Протокол Диффи-Хеллмана.	4	[5]
8	Эллиптические кривые в криптографии.	4	[5]
9	Генерирование случайных чисел.	2	[10]
10	Шифр эль-Гамала.	4	[11]
11	Цифровая подпись.	5	[12]
Итого:		51	

3.5. Самостоятельная работа студента

№ п/п	Виды самостоятельной работы студента	Объем, час.
1	Изучение лекционного материала	34
2	Подготовка к лабораторным работам	31
Итого:		61

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В процессе изучения дисциплины применяются следующие виды контроля:

1) Текущее тестирование или текущий опрос по изученным темам программы. Текущее тестирование или текущий опрос проводится во время лекционных, практических и лабораторных занятий, также учитывается качество и своевременность выполнения и сдачи соответствующей лабораторной работы.

2) Оценка качества и своевременность выполнения заданий, относящихся к соответствующей теме.

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.

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

5. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Литература:

Основная:

1. Мельников, В.П. Информационная безопасность и защита информации / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - М. : ИЦ "Академия", 2009. - 336с.
2. Куприянов, А.И. Основы защиты информации : учебное пособие для вузов / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов ; А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. - 3-е изд., стер. - М. : ИЦ "Академия", 2008. - 256с. - (Высшее профессиональное образование. Радиоэлектроника).
3. Рябко, Б. Я. Основы современной криптографии и стеганографии [Электронный ресурс]. - М. : Горячая линия-Телеком, 2010. - 232 с.
4. Герман, О. Н. Теоретико-числовые методы в криптографии: учебник для студентов учреждений высшего профессионального образования, обучающихся по направлениям подготовки "Информационная безопасность" и "Математика" / О. Н. Герман, Ю. В. Нестеренко. - Москва: Академия, 2012. - 272 с.
5. Романьков, В. А. Введение в криптографию: курс лекций / В. А. Романьков. - 2-е изд., испр. и доп. - М.: Форум, 2012. - 240 с.
6. Гашков, С. Б. Криптографические методы защиты информации : учеб. пособие для студ. вузов. - М.: Академия, 2010.
7. Басалова, Г.В. Основы криптографии [Электронный ресурс] : [курс лекций] / Г. В. Басалова. - 66 Мб. - М. : ИНТУИТ, 2016. - 1 файл. - Систем. требования: Acrobat Reader.
8. Мир математики: в 40 т. Т. 2: Жуан Гомес. Математики, шпионы и хакеры. Кодирование и криптография. [Электронный ресурс] / Жуан Гомес. – М.: Де Агостини, 2014. – 144 с. – 56,1 Мб. - 1 файл. - Систем. требования: Acrobat Reader.
9. Сингх, С. Книга тайных шифров и их расшифровки / Саймон Сингх. – М.: АСТ: Астрель, 2007. – 447с. – 11, 1 Мб. - 1 файл. - Систем. требования: Просмотрщик djvu-файлов.
10. Методические рекомендации для самостоятельной работы студентов нормативной учебной дисциплины цикла естественно-научной и общеэкономической подготовки "Криптографии и стеганография" = Методичні рекомендації для самостійної роботи студентів з нормативної навчальної дисципліни циклу природничо-наукової та загальноєкономічної підготовки "Криптографія та стеганографія" [Електронний ресурс] : галузь знань: 1701 Інформаційна безпека : напрям підготовки: 6.170100 Захист інформації з обмеженим доступом та автоматизація її обробки / 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. О.В. Оводенко. - 52 Мб. - Донецьк : ДВНЗ "ДонНТУ", 2010. - 1 файл. - Систем. вимоги: Acrobat Reader.

11. Методические рекомендации для самостоятельной работы студентов дисциплины цикла "Основы прикладной криптологии" = Методичні рекомендації для самостійної роботи студентів з навчальної дисципліни циклу "Основы прикладної криптології" [Електронний 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. О.В. Оводенко. - 52 Мб. - Донецьк : ДВНЗ "ДонНТУ", 2013. - 1 файл. - Систем. вимоги
12. Методические указания к выполнению лабораторных работ по дисциплине «Криптография и стеганография» - Донецк: ДонНТУ.

Составитель рабочей программы: _____ А.В.Оводенко
(подпись)