МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
"Курский государственный университет"

Кафедра информационной безопасности

УТВЕРЖДЕНО

протокол заседания
Ученого совета от 24.04.2017 г., №10

Рабочая программа дисциплины
Криптографические методы защиты информации

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 3 ЗЕТ

Виды контроля в семестрах:

зачет(ы) с оценкой 7

курсовой проект 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	36	36	36	36
Итого ауд.	54	54	54	54
Контактная работа	54	54	54	54
Сам. работа	54	54	54	54
Итого	108	108	108	108

Курск 2017

Рабочая программа дисциплины Криптографические методы защиты информации / сост. ; Курск. гос. ун-т. - Курск, 2017. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 1 декабря 2016 г. № 1515 "Об утверждении ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата)" (Зарегистрировано в Минюсте России 20 декабря 2016 г. № 44821)

Рабочая программа дисциплины "Криптографические методы защиты информации" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Ознакомление с основами математической теории методов криптозащиты и криптоанализа. Приобретение навыков в практическом использовании современных алгоритмов криптопреобразования и криптоанализа.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.Б

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-1: Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Знать:
понятие составляющие и проблемы информационной безопасности;
объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные и аппаратные средства
нормативно-правовые, экономические и технологические методы обеспечения информационной безопасности.
Уметь:
обосновать и сформулировать решения по применению технологических и нормативно-правовых средств и методов обеспечения информационной безопасноти
Применять криптогргфические и информационно-аналитические системы, информационные ресурсы и информационные технологии
Сформулировать основные криптографические методы и методы стеганографии
Владеть:
Методом дискретного логарифмирования в конечных циклических группах
Методом применения основных криптосистем и систем стеганографирования
Методом применения алгоритмов проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах

ПК-2: Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
Знать:
программные средства системного, прикладного и специального назначения
инструментальные средства, язык и системы программирования
основные проблемы применения программных средств, системного прикладного и специального назначения
Уметь:
применять программные средства системного, прикладного и специального назначения
применять инструментальные средства, язык и системы программирования
применять методы решения основных проблем при применении программных средств, системного прикладного и специального назначения
Владеть:
Навыками применения программных средств системного, прикладного и специального назначения
Навыками применения инструментальных средств, языка и системы программирования
Навыками применения методов решения основных проблем при применении программных средств, системного прикладного и специального назначения

ПК-7: Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
Знать:
методы и способы получения хранения и переработки информации, структуру локальных и глобальных компьютерных сетей
основные понятия математической логики и теории алгоритмов;
основные понятия и методы дискретной математики, включая дискретные функции, конечные автоматы, комбинаторный анализ;
Уметь:
Сформулировать основные методы и способы получения хранения и переработки информации, структуру локальных и глобальных компьютерных сетей
Применять основные дискретные структуры, используемые в компьютерных системах, структуру локальных и глобальных компьютерных сетей;

Применять технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми
Владеть:
Навыками использования основных методов и способов получения хранения и переработки информации, структуру локальных и глобальных компьютерных сетей
Навыками сбора и анализа исходных данных для проектирования систем защиты информации, а так же определением требований и сравнительным анализом подсистем по показателям информационной безопасности.
Методом проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интеракт.
	Раздел 1. Раздел 1. Введение в криптографию	Раздел			
1.1	Введение в криптографию История криптографии. Криптостойкость. Теория вероятности и криптогра-фия	Лек	7	2	0
1.2	Практическая работа №1	Лаб	7	4	0
1.3	Симметричные шифры. Поточные шифры. Блочные шифры	Лек	7	1	0
1.4	Симметричные шифры. Поточные шифры. Блочные шифры	Ср	7	12	0
1.5	Практическая работа №2	Лаб	7	4	0
1.6	Изучение криптосистемы DES. Распределение симметричных ключей. Разделение секрета	Лек	7	2	0
1.7	Практическая работа №3	Лаб	7	4	0
1.8	Арифметика остатков. Односторонние функции. Алгоритм RSA.	Лек	7	2	0
1.9	Практическая работа №4	Лаб	7	4	0
1.10	Криптосистема Эль-Гамаль. Криптосистема Рабина. Схемы цифровой подписи: 1) RSA, 2) DSA, Хэш-функция	Лек	7	2	0
1.11	Практическая работа №5	Лаб	7	4	0
1.12	Псевдослучайные последовательности и поточные шифры	Лек	7	1	0
1.13	Практическая работа №6	Лаб	7	4	0
1.14	Определение теоретической стойкости алгоритма. Шифр Вернама для 8-битных символов. Побитный «одноразовый блокнот». Виды атак. Понятие о практической стойкости шифра. Временная стой-кость шифра	Лек	7	2	0
1.15	Практическая работа №7	Лаб	7	4	0
1.16	Криптографические системы, основанные на физи-ческих принципах защиты информации. Квантовая криптография	Лек	7	2	0
1.17	Практическая работа №8	Лаб	7	4	0
1.18	Стеганогрфический метод защиты информации	Лек	7	4	0
1.19	Рубежный контроль	Лаб	7	4	0
1.20	Самостоятельная работа №1	Ср	7	8	0
1.21	Самостоятельная работа №2	Ср	7	8	0
1.22	Самостоятельная работа №3	Ср	7	8	0
1.23	Самостоятельная работа №4	Ср	7	8	0
1.24	Самостоятельная работа №5	Ср	7	8	0
1.25	Промежуточный контроль	ЗачётСОц	7	2	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине "Криптографические методы защиты информации" были рассмотрены и одобрены на заседании кафедры "Программного обеспечения и администрирования информационных систем " от 30 марта 2017 г., протокол №8"

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточной аттестации по дисциплине "Криптографические методы защиты информации" были рассмотрены и одобрены на заседании кафедры "Программного обеспечения и администрирования информационных систем " от 30 марта 2017 г., протокол №8"

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Заглавие	Эл. адрес	Кол-
Л1.1	Лапонина О. Р. - Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия: учебное пособие - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.	http://www.iprbookshop.ru/22432	1
Л1.2	Фомичёв В. М. - Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: Учебник - М.: Издательство Юрайт, 2017.	http://www.biblio-online.ru/book/C0328DC2-2A46-4945-994F-04F661095B83	1
Л1.3	Смирнов А.Э., Пономарёва Ю.А. - Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации: практикум - Москва: Московский технический университет связи и информатики, 2015.	http://www.iprbookshop.ru/61738.html	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-
Л2.1	Бехроуз А. - Криптография и безопасность сетей: учебное пособие - Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.	http://www.iprbookshop.ru/72337.html	1

6.3.1 Перечень программного обеспечения

7.3.1.1	198:
7.3.1.2	MacOS 10.11(Документы о приобре-тении iMac 21.5")
7.3.1.3	OracleVMVirtualBox (Свободная ли-цензия GNUGPL 2)
7.3.1.4	Microsoft Windows 7 (Open License: 47818817)
7.3.1.5	MsOffice Professional 2007 (Open Li-cense: 43219389)
7.3.1.6	Adobe Acrobat Reader DC (Бесплатное программное обеспечение)
7.3.1.7	7-Zip (Свободная лицензия GNULGPL)
7.3.1.8	GoogleChrome (Свободная лицензия BSD)
7.3.1.9	FlatAssembler (Свободное программ-ное обеспечение лицензия BSD с воз-можно анти-GPL)
7.3.1.10	VisualStudioCommunity (Проприетар-ная академическая лицензия)
7.3.1.11	Code::Blocks (Свободная лицензия GNUGPLv3)
7.3.1.12	EclipseNeon (Открытое программное обеспечение EclipsePublicLicense)
7.3.1.13	
7.3.1.14	146:
7.3.1.15	Microsoft Windows 7 (OpenLi-cense: 47818817)
7.3.1.16	Ms OfficeProfessional 2007 (OpenLicense: 47818817
7.3.1.17	Google Chrome (Свободная ли-цензия BSD)

7.3.1.18	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.19	Adobe Acrobat Reader DC (Бес-платное программное обеспе-чение)
6.3.2 Перечень информационных справочных систем	
7.3.2.1	Каталог библиотеки КГУ. - Режим доступа: http://195.93.165.10:2280
7.3.2.2	Электронная библиотека.- Режим доступа: http://elibrary.ru
7.3.2.3	Университетская информационная система «Россия» – http://uisrussia.msu.ru
7.3.2.4	Электронная библиотечная система «КнигаФонд» − http://www.knigafund.ru/
7.3.2.5	Электронная библиотечная система «IPRbooks» − http://www.iprbookshop.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Компьютерная аудитория для проведения занятий лекцион-ного типа, занятий семинарско-го типа, групповых и индиви-дуальных консультаций, курсо-вого проектирования (выпол-нения курсовых работ), само-стоятельной работы студентов, текущего контроля и промежу-точной аттестации,
7.2	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 198.
7.3	Интерактивная доска – 1 шт.
7.4	Доска Классная – 1 шт.
7.5	Applei Mac 21.5 – 15 шт.
7.6	Коммутатор 24порт. – 1 шт.
7.7	
7.8	Помещение для самостоятельной работы обучающихся – аудитория, оснащенная компьютерной техни-кой с возможностью подключения к сети "Интернет" и с обеспечени-ем доступа в электронную инфор-мационно-образовательную среду университета.
7.9	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 146.
7.10	Столов – 61
7.11	Посадочных мест – 162
7.12	Компьютеров:
7.13	Для пользователей – 40
7.14	Для библиотекаря – 2
7.15	Моноблоков MSI (27) - модель MS-A912, 2гб оперативной памя-ти, Athlon CPU D525 1.80GHz
7.16	Моноблоков Asus (13) - модель ET2220I, 4гб оперативной памяти, Intel Core i3-3220 CPU 3.30 GHz

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Студентам необходимо ознакомиться с содержанием рабочей программы, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками, имеющимся на кафедре.

1.1. Указания по подготовке к занятиям лекционного типа

Изучение дисциплины требует систематического и последовательного накопления знаний, поэтому студентам рекомендуется перед очередной лекцией просмотреть по конспекту материал предыдущей. При затруднениях в восприятии материала следует обращаться к основным литературным источникам, к лектору (по графику его консультаций) или к преподавателю на занятиях семинарского типа.

1.2. Указания по подготовке к лабораторным занятиям

Лабораторные занятия имеют следующую структуру:

- тема занятия;
- цели проведения занятия по соответствующим темам;
- задания состоят из выполнения практических заданий, примеров;
- рекомендуемая литература.

«Методические указания по подготовке к практическим занятиям по дисциплине «Криптографические методы защиты информации» утверждены на заседании кафедры от 30 марта 2017 г., протокол №8", находятся на кафедре «Программного обеспечения и администрирования информационных систем» в свободном доступе для студентов.

1.3. Методические указания по выполнению самостоятельной работы

Самостоятельная работа студентов включает в себя выполнение практических заданий, самостоятельное изучение отдельных вопросов по теме. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы, которые содержатся в «Методических указаниях по самостоятельной работе по дисциплине «Криптографические методы защиты информации»», утвержденных на заседании кафедры от 30 марта 2017 г., протокол

№8"
и находятся на кафедре « Программного обеспечения и администрирования информационных систем» в свободном доступе для студентов.

1.4. Методические указания по работе с литературой

Основная литература к данной дисциплине - это учебники и учебные пособия.
Дополнительная литература - это монографии, сборники научных трудов, журнальные и газетные статьи, различные справочники, энциклопедии, интернет ресурсы.

В учебнике/ учебном пособии/ монографии следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие. Целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения. Такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, а какие прочитать быстро.
Студенту следует использовать следующие виды записей при работе с литературой:
Конспект - краткая схематическая запись основного содержания научной работы. Целью является не переписывание произведения, а выявление его логики, системы доказательств, основных выводов.
Цитата - точное воспроизведение текста. Заключается в кавычки. Точно указывается страница источника.
Тезисы - концентрированное изложение основных положений прочитанного материала.
Аннотация - очень краткое изложение содержания прочитанной работы.
Резюме - наиболее общие выводы и положения работы, ее концептуальные итоги и другие виды.