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
Математические основы криптологии

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 5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	36	36	36	36
В том числе инт.	20	20	20	20
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 Математические основы криптологии / сост. к.т.н., доцент, Крыжевич Л.С.; 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 "Математические основы криптологии" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

к.т.н., доцент, Крыжевич Л.С.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	является фундаментализация образования студентов, формирование у них научного мировоззрения и системного мышления, ценностно-информационного подхода к анализу и синтезу защищенных систем связи, приобретение фундаментальных знаний, умений и навыков по вероятностному и статистическому анализу потоков данных, моделированию защищенных протоколов передачи информации, проведению расчетов криптостойкости, оценке пределов применимости электронных цифровых подписей и различных криптосистем.

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

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОПК-2: Способностью применять соответствующий математический аппарат для решения профессиональных задач
Знать:
использовать методы дискретной математики при решении практических задач криптографии
Уметь:
оценивать скорость передачи информации и пропускную способность каналов передачи информации при отсутствии и наличии помех, а также применять знания о кодах, корректирующие ошибки;
Владеть:
использовать типовые методы криптографического анализа

ПСК-1.2: Способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований
Знать:
Уметь:
Владеть:

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интеракт.
	Раздел 1. Алгебро-геометрические основы криптографии	Раздел			
1.1	Теория делимости	Лек	5	4	2
1.2	Алгебро-геометрические основы криптографии	Пр	5	6	2
1.3	Криптосистемы на основе модулярной арифметики	Лек	5	2	0
1.4	Модулярная арифметика	Пр	5	6	2
1.5	Элементы высшей алгебры	Лек	5	2	2
1.6	Аффинные криптосистемы	Пр	5	4	2
1.7	Аффинные криптосистемы	Ср	5	7	0
1.8	Элементы алгебраической геометрии	Лек	5	2	2

1.9	Факторизация простых чисел	Ср	5	18	0
1.10	Текущий контроль	Пр	5	2	0
	Раздел 2. Математические основы построения криптопротоколов	Раздел			
2.1	Вероятностно-статистические основы кодирования	Лек	5	2	0
2.2	Ассимметричные криптосистемы	Пр	5	6	2
2.3	Методы статистического тестирования случайных и псевдослучайных последовательностей	Лек	5	2	2
2.4	Электронная цифровая подпись	Пр	5	6	2
2.5	Методы криптоанализа	Лек	5	2	0
2.6	Эллиптические кривые	Пр	5	4	2
2.7	Квантовая криптография	Ср	5	27	0
2.8	Криптография на булевых функциях	Лек	5	2	0
2.9	Текущий контроль	Пр	5	2	0
2.10	Промежуточный контроль	ЗачётСОц	5	2	0

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине "Математические основы криптологии" рассмотрены и одобрены на заседании кафедры программного обеспечения и администрирования информационных систем от «30» марта 2017 г. протокол № 8, является приложением к рабочей программе.

5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточной аттестации по дисциплине "Математические основы криптологии" рассмотрены и одобрены на заседании кафедры программного обеспечения и администрирования информационных систем от «30» марта 2017 г. протокол № 8, является приложением к рабочей программе.

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Заглавие	Эл. адрес	Кол-
Л1.1	Щеглов А. Ю. - Защита информации: основы теории: Учебник - М.: Издательство Юрайт, 2017.	http://www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E	1
Л1.2	Данилова Т. В. - Теория чисел: Задачи с примерами решений - Архангельск: САФУ, 2015.	http://biblioclub.ru/index.php?page=book&id=436368	1
Л1.3	Фирдман И. А. - Теоретико-числовые алгоритмы и их применение в криптографии - Омск: Омский государственный университет, 2011.	http://biblioclub.ru/index.php?page=book&id=238201	1

6.1.2. Дополнительная литература

	Заглавие	Эл. адрес	Кол-
Л2.1	Кочергин В. И. - Практика теории многомерных цифро-векторных множеств (криптология) - Томск: Изд-во Томского ун-та, 2011.	ftp://192.168.131.48/EBOOKS/001.pdf	1
Л2.2	Фомичев В.М. - Дискретная математика и криптология: Курс лекций - М.: ДИАЛОГ-МИФИ, 2003.		4

6.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Windows Win10Pro (64) (акт приема-передачи товара от 31 июля 2017, контракт №0344100007517000020 -0008905-01)
7.3.1.2	MsOffice Professional 2007 (Open License: 43219389)
7.3.1.3	Adobe Acrobat Reader DC (Бесплатное программное обеспечение)
7.3.1.4	7-Zip (Свободная лицензия GNU LGPL)
7.3.1.5	GoogleChrome (Свободная лицензия BSD)
7.3.1.6	MATLAB 7 (Сублицензионный договор № 43/ЗЦт «4 » апреля 2018 г.)

6.3.2 Перечень информационных справочных систем

7.3.2.1	Каталог библиотеки КГУ. - Режим доступа: http://195.93.165.10:2280, свободный.- Яз. рус., англ.
7.3.2.2	Электронная библиотека.- Режим доступа: http://elibrary.ru, с экрана.- Яз. рус., англ.
7.3.2.3	http://uisrussia.msu.ru – Университетская информационная система «Россия»
7.3.2.4	Электронная библиотечная система «КнигаФонд» − http://www.knigafund.ru/
7.3.2.5	Электронная библиотечная система IPRbooks − www.iprbookshop.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Лаборатория автоматического проектирования и моделирования : учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа,
7.2	групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы,
7.3	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 193.
7.4	Комплекты учебных столов и стульев (10 шт);
7.5	Комплекты компьютерных столов и стульев (10 шт),
7.6	Доска классная,
7.7	Компьютер в сборе DellOptPlexMT3050 – 12 шт.
7.8	Концентратор 16-портовый – 1 шт.
7.9	
7.10	Помещение для самостоятельной работы обучающихся – аудитория, оснащенная компьютерной техникой с возможностью подключения к сети "Интернет" и с обеспечением доступа в электронную информационно-образовательную среду университета.
7.11	305000, Курская область, г. Курск, ул. Радищева д. № 33, 146.
7.12	Столов – 61
7.13	Посадочных мест – 162
7.14	Компьютеров:
7.15	Для пользователей – 40
7.16	Для библиотекаря – 2
7.17	Моноблоков MSI (27) - модель MS-A912, 2гб оперативной памяти, Athlon CPU D525 1.80GHz
7.18	Моноблоков Asus (13) - модель ET2220I, 4гб оперативной памяти, IntelCore 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 занятиям семинарского типа

Практические занятия имеют следующую структуру:

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

1.3. Методические указания по выполнению самостоятельной работы

Самостоятельная работа студентов включает в себя выполнение практических заданий, самостоятельное изучение отдельных вопросоы по теме. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы.

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.