ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.03.02 Математические основы криптографии

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Квалификация выпускника специалист

Форма обучения очная

1. Цели освоения дисциплины

Целями освоения дисциплины «Математические основы криптографии» являются:

- формирование теоретических знаний основных криптографических алгоритмов и практических навыков их применения для защиты информации;
- изучение основных положений криптографии, ознакомление с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами, электронной подписью.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Математические основы криптографии» относится к вариативной части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Математические основы криптографии» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ПК-2	Организация ЭВМ и вычислительных систем Учебная практика (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ПК-2	Моделирование систем 3D-моделирование Производстненная научно-исследовательская работа Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ПК-2 - способностью создавать и исследовать модели автоматизированных систем	Этап 1: базовые понятия основ моделирования	Этап 1: использовать методы моделирования для создания моделей	Этап 1: использования методов моделирования для создания моделей
ПК-2 - способностью создавать и исследовать модели	Этап 2: модели автоматизированны х систем	Этап 2: использовать структурные	Этап 2: использования структурных моделей

автоматизированных систем		модели	

4. Объем дисциплины

Объем дисциплины «Математические основы криптографии» составляет 2 зачетных единиц (72 академических часа), распределение объема дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

№ п/п	Вид учебных занятий	Итого КР	Итого СР	Семестр № 5	
				КР	СР
1	**2**	**3**	**4**	**5**	**6**
1	Лекции (Л)	16	-	16	-
2	Лабораторные работы (ЛР)	16	-	16	-
3	Практические занятия (ПЗ)	16	-	16	-
4	Семинары(С)	-	-	-	-
5	Курсовое проектирование (КП)	-	-	-	-
6	Рефераты (Р)	-	-	-	-
7	Эссе (Э)	-	-	-	-
8	Индивидуальные домашние задания (ИДЗ)	-	-	-	-
9	Самостоятельное изучение вопросов (СИВ)	-	10	-	10
10	Подготовка к занятиям (ПкЗ)	-	12	-	12
11	Промежуточная аттестация	2		2	
12	Наименование вида промежуточной аттестации	x	x	зачет	
13	Всего	50	22	50	22

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1 – Структура дисциплины

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	**Раздел 1 Введение. Стойкость криптографических систем и алгоритмов.**	**5**	**4**	**4**	**4**	**-**	**-**	**x**	**-**	**4**	**4**	**x**	**ПК-2**
1.1.	**Тема 1** Основные понятия и определения. История развития криптографии. Законодательные и правовые основы защиты компьютерной информации и информационных технологий.	5	2	2	2	-	-	x	-	2	2	x	ПК-2
1.2.	**Тема 2** Энтропия, теоретическая и практическая стойкость, вычислительная стойкость.	5	2	2	2	-	-	x	-	2	2	x	ПК-2
2	**Раздел 2 Современные симметричные криптосистемы. Распределение ключей.**	**5**	**4**	**4**	**4**	**-**	**-**	**x**	**-**	**2**	**4**	**x**	**ПК-2**
2.1	**Тема 3** Блочные и поточные шифры. Шифры DES, режимы работы DES, AES, ГОСТ 28147-89.	5	2	2	2	-	-	x	-	2	2	x	ПК-2

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
2.2	**Тема 4** Поточные шифры: РСЛОС, RC4, шифр Рона.	5	2	2	2	-	-	х	-	-	2	х	ПК-2
3.	**Раздел 3** **Асимметричные криптосистемы.**	**5**	**4**	**4**	**4**	**-**	**-**	**х**	**-**	**2**	**2**	**х**	**ПК-2**
3.1	**Тема 5** Общая схема функционирования систем с открытыми ключами.	5	2	2	2	-	-	х	-	2	-	х	ПК-2
3.2	**Тема 6** Криптосистема RSA и ее модификации. Криптосистема Эль Гамаля. Криптосистема Рабина. Электронная цифровая подпись.	5	2	2	2	-	-	х	-	-	2	х	ПК-2
4.	**Раздел 4** **Криптографические протоколы.**	**5**	**4**	**4**	**4**	**-**	**-**	**х**	**-**	**2**	**2**	**х**	**ПК-2**
4.1	**Тема 7** Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля. Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний. Схемы обязательств. Системы электронного голосования. Цифровые сертификаты: системы перераспределения доверия, неявные сертификаты.	5	2	2	2	-	-	х	-	-	2	х	ПК-2

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
4.2	**Тема 8** Тесты на простоту и факторизация. Надежность криптосистем. Элементы криптоанализа.	5	2	2	2	-	-	x	-	2	-	x	ПК-2
5.	**Контактная работа**	**5**	**16**	**16**	**16**	**-**	**-**	**x**	**-**	**-**	**-**	**2**	**x**
6.	**Самостоятельная работа**	**5**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**10**	**12**	**-**	**x**
7.	**Объем дисциплины в семестре**	**5**	**16**	**16**	**16**	**-**	**-**	**-**	**-**	**10**	**12**	**2**	**x**
8.	**Всего по дисциплине**	**x**	**16**	**16**	**16**	**-**	**-**	**-**	**-**	**10**	**12**	**2**	**x**

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Основные понятия и определения. История развития криптографии. Законодательные и правовые основы защиты компьютерной информации и информационных технологий.	2
Л-2	Энтропия, теоретическая и практическая стойкость, вычислительная стойкость.	2
Л-3	Блочные и поточные шифры. Шифры DES, режимы работы DES, AES, ГОСТ 28147-89.	2
Л-4	Поточные шифры: РСЛОС, RC4, шифр Рона.	2
Л-5	Общая схема функционирования систем с открытыми ключами.	2
Л-6	Криптосистема RSA и ее модификации. Криптосистема Эль Гамаля. Криптосистема Рабина. Электронная цифровая подпись.	2
Л-7	Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля. Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний. Схемы обязательств. Системы электронного голосования. Цифровые сертификаты: системы перераспределения доверия, неявные сертификаты.	2
Л-8	Тесты на простоту и факторизация. Надежность криптосистем. Элементы криптоанализа.	2
Итого по дисциплине		16

5.2.2 – Темы лабораторных работ

№ п.п.	Наименование темы лабораторной	Объем, академические часы
ЛР-1	Поточные системы шифрования (РСЛОС, RC4, Рона)	2
ЛР-2	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)	2
ЛР-3	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	2
ЛР-4	Асимметричные криптосистемы (RSA, El Gamal, Рабина)	2
ЛР-5-6	Программная реализация асимметричных криптосистем (RSA, El Gamal, Рабина)	4
ЛР-7-8	Исследование тестов на простоту и алгоритмы факторизации.	4
Итого по дисциплине		16

5.2.3 – Темы практических занятий

№ п.п.	Наименование темы занятия	Объем, академические часы
ПЗ-1	Поточные системы шифрования (РСЛОС, RC4, Рона)	2
ПЗ-2	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)	2
ПЗ-3	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	2
ПЗ-4	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	2
ПЗ-5	Асимметричные криптосистемы (***RSA***, El Gamal, Рабина) Формирование ассиметричных криптосистем	2
ПЗ-6	Асимметричные криптосистемы (***RSA***, El Gamal, Рабина) Формирование ассиметричных криптосистем RSA	2
ПЗ-7	Асимметричные криптосистемы (***RSA***, El Gamal, Рабина) Формирование ассиметричных криптосистем Рабина	2
ПЗ-8	Асимметричные криптосистемы (***RSA***, El Gamal, Рабина) Формирование ассиметричных криптосистем El Gamal	2
Итого по дисциплине		16

5.2.4 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Основные понятия и определения. История развития криптографии. Законодательные и правовые основы защиты компьютерной информации и информационных технологий	Законодательные и правовые основы защиты компьютерной информации и информационных технологий	2
2.	Энтропия, теоретическая и практическая стойкость, вычислительная стойкость.	Модульная арифметика	2
3.	Блочные и поточные шифры. Шифры DES, режимы работы DES, AES, ГОСТ 28147-89.	Схемы обмена секретными ключами: широкоротой лягушки, Ниджейма-Шредера, Отвэй-Риса	2
4.	Общая схема функционирования систем с открытыми ключами.	Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний.	2

5.	Тесты на простоту и факторизация. Надежность криптосистем. Элементы криптоанализа.	Элементы криптоанализа.	2
Итого по дисциплине			10

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 c.

2. Бескид П.П. Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс]: учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— СПб.: Российский государственный гидрометеорологический университет, 2010.— 95 c.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Авдошин С.М., Сердюк В.А., Савельева А.А. Технологии и продукты Microsoft в обеспечении информационной безопасности. Издательство: Интернет-Университет Информационных Технологий, 2010 г.- 455 с..
2. Сидельников В.М. Теория кодирования. Издательство: ФИЗМАТЛИТ, 2011 г.- 323 с.-

6.3 Методические материалы для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие, включающее:

- конспект лекций;
- методические материалы по выполнению лабораторных работ;
- методические материалы по выполнению практических (семинарских) работ.

6.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Электронное учебное пособие включающее:

- методические рекомендации по самостоятельному изучению вопросов;
- методические рекомендации по подготовке к занятиям.

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. JoliTest
2.Open Office

6.6 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://www.intuit.ru/studies/courses/
2. http://www.fstec.ru/
3. https://rkn.gov.ru/

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиапроектором, компьютером, учебной доской.

Таблица 7.1 – Материально-техническое обеспечение практических занятий

Вид и номер занятия	Тема занятия	Название специализированной аудитории	Название оборудования	Название технических и электронных средств обучения и контроля знаний
ПЗ-1	Практические занятия в соответствии с рабочей программой	941-Лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-2	Практические занятия в соответствии с рабочей программой	941-Лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-3	Практические занятия в соответствии с рабочей программой	941-Лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-4	Практические занятия в соответствии с рабочей программой	941-Лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, укомплектованных специализированной мебелью и техническими средствами обучения.

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций, укомплектованных специализированной мебелью и техническими средствами обучения.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.

Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованном специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Разработал(и): _____ Боровский А.С.