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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.1.26 Криптографические методы защиты информации

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:

- формирование у студентов знаний теории и методов защиты информации путем криптографической защиты сообщений, осуществления секретной связи на основе симметричных и асимметричных криптосистем, а также методов реализации электронной (цифровой) подписи;

- раскрытие возможностей и особенностей криптографии и криптоанализа применительно к задачам проектирования защищенных систем и сетей связи и передачи данных.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Криптографические методы защиты информации» относится к базовой части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Криптографические методы защиты информации» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ОК-5	Основы информационной безопасности Социология
ПК-14	Метрология и электро-радиоизмерения 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
ОК-5	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-14	Технология защиты информации в различных отраслях деятельности Системы обнаружения вторжений Производственная практика по получению профессиональных умений и опыта профессиональной деятельности Системы предотвращения утечек 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
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 1: Цели, задачи, принципы и основные направления обеспечения криптографической информационной безопасности государства	Этап 1: Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня защиты с учетом криптографических средств защиты информации	Этап 1: Профессиональной терминологией и методами теоретического обоснования в выборе криптографических средств обеспечения информационной безопасности
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 2: Современные подходы к построению криптографических систем защиты информации	Этап 2: Применять отечественные и зарубежные стандарты в области компьютерной безопасности с использованием криптографических средств обеспечения информационной безопасности.	Этап 2: Владеть методологическим и принципами оценки защищенности объектов информатизации и обеспечения требуемого уровня защиты с использованием криптографических средств обеспечения информационной безопасности
ПК-14 – способностью проводить контрольные проверки работоспособности применяемых программно аппаратных, криптографических и технических средств защиты информации	Этап 1: основные этапы контрольных проверок технических средств защиты информации	Этап 1: разрабатывать методику контрольных проверок технических средств защиты информации	Этап 1: навыки применения контрольных проверок;

ПК-14 – способностью проводить контрольные проверки работоспособности применяемых программно аппаратных, криптографических и технических средств защиты информации	Этап 2: основные принципы работы технических средств защиты информации	Этап 2: разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации	Этап 2: навыки оценки эффективности применении аппаратно - программных комплексов

4. Объем дисциплины

Объем дисциплины «Криптографические методы защиты информации» составляет 5 зачетных единиц (180 академических часов), 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 № 6	
				КР	СР
1	**2**	**3**	**4**	**5**	**6**
1	Лекции (Л)	38		38	
2	Лабораторные работы (ЛР)	18		18	
3	Практические занятия (ПЗ)	18		18	
4	Семинары(С)				
5	Курсовое проектирование (КП)				
6	Рефераты (Р)				
7	Эссе (Э)				
8	Индивидуальные домашние задания (ИДЗ)				
9	Самостоятельное изучение вопросов (СИВ)		30		30
10	Подготовка к занятиям (ПкЗ)		72		72
11	Промежуточная аттестация	4		4	
12	Наименование вида промежуточной аттестации	х	х	экзамен	
13	Всего	78	102	78	102

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**	6	8	4	4			x		8	18	x	ОК-5 ПК-14
1.1.	**Тема 1** Классификация криптографических систем	6	4	2	2			x		4	8	x	ОК-5 ПК-14
1.2.	**Тема 2** Простые шифры и их свойства	6	4	2	2			x		4	10	x	ПК-14
2.	**Раздел 2 Современные симметричные криптосистемы. Распределение ключей**	6	10	6	6			x		8	18	x	ОК-5 ПК-14
2.1.	**Тема 3** Симметричные системы шифрования (системы шифрования с секретным ключом)	6	4	4	4			x		4	8	x	ОК-5

№ 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** Системы шифрования с открытым ключом	6	6	2	2			x		4	10	x	ОК-5 ПК-14
3.	**Раздел 3 Асимметричные криптосистемы**	6	10	4	4			x		8	18	x	ОК-5 ПК-14
3.1.	**Тема 5** Общая схема функционирования систем с открытыми ключами	6	4	2	2			x		4	10	x	ОК-5 ПК-14
3.2.	**Тема 6** Криптосистема RSA и ее модификации	6	6	2	2			x		4	8	x	ОК-5
4.	**Раздел 4 Криптографические протоколы**	6	10	4	4			x		6	18	x	ОК-5 ПК-14
4.1.	**Тема 7** Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля	6	4	2	2			x		4	8	x	ПК-14

№ 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	6	6	2	2			x		2	10	x	ОК-5 ПК-14
5.	**Контактная работа**	6	38	18	18			x				4	x
6.	**Самостоятельная работа**	6						x		30	72		x
7.	**Объем дисциплины в семестре**	6	38	18	18			x		30	72	4	x
8.	**Всего по дисциплине**	x	38	18	18			x		30	72	6	x

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Введение	**2**
Л-2	Законодательные и правовые основы защиты компьютерной информации и информационных технологий	**2**
Л-3	Законодательные и правовые основы защиты компьютерной информации и информационных технологий	**2**
Л-4	Стойкость криптографических систем и алгоритмов	**2**
Л-5	Вычислительные алгоритмы	**2**
Л-6	Вычислительные алгоритмы	**2**
Л-7	Блочные и поточные шифры	**2**
Л-8	Шифры DES, режимы работы DES, AES, ГОСТ 28147-89	**2**
Л-9	Шифры DES, режимы работы DES, AES, ГОСТ 28147-89	**2**
Л-10	Поточные шифры: РСЛОС, RC4, шифр Рона	**2**
Л-11	Распределение ключей	**2**
Л-12	Общая схема функционирования систем с открытыми ключами	**2**
Л-13	Криптосистема RSA и ее модификации. Криптосистема Эль Гамаля. Криптосистема Рабина	**2**
Л-14	Целостность данных и аутентификация сообщений	**2**
Л-15	Хэш-функции	**2**
Л-16	«Реализация схем электронной цифровой подписи (на основе алгоритмов RSA, El Gamal, Шнорра)».	**2**
Л-17	«Реализация схем электронной цифровой подписи (на основе алгоритмов RSA, El Gamal, Шнорра)»	**2**
Л-18	«Криптографические протоколы»	**2**
Л-19	«Тесты на простоту и факторизация».	**2**
Итого по дисциплине		**38**

5.2.2 – Темы лабораторных работ

№ п.п.	Наименование темы занятия	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	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	**2**
ЛР -5	Асимметричные криптосистемы (RSA, El Gamal, Рабина)	**2**
ЛР -6	Асимметричные криптосистемы (RSA, El Gamal, Рабина)	**2**
ЛР -7	Программная реализация асимметричных криптосистем (RSA, El Gamal, Рабина)	**2**
ЛР -8	Программная реализация асимметричных криптосистем (RSA, El Gamal, Рабина)	**2**
ЛР -9	Программная реализация асимметричных криптосистем (RSA, El Gamal, Рабина)	**2**
Итого по дисциплине		**18**

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	Поточные системы шифрования (РСЛОС, RC4, Рона)	**2**
ПЗ-3	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)	**2**
ПЗ-4	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)	**2**
ПЗ-5	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	**2**
ПЗ-6	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	**2**
ПЗ-7	Асимметричные криптосистемы (***RSA***, ElGamal, Рабина) Формирование ассиметричных криптосистем	**2**
ПЗ-8	Асимметричные криптосистемы (***RSA***, ElGamal, Рабина) Формирование ассиметричных криптосистем	**2**
ПЗ-9	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	**2**
Итого по дисциплине		**18**

5.2.4 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Классификация криптографических систем.	Законодательные и правовые основы защиты	4

		компьютерной информации и информационных технологий	
2.	Простые шифры и их свойства.	Модульная арифметика	4
3.	Симметричные системы шифрования (системы шифрования с секретным ключом).	Схемы обмена секретными ключами: широкоротой лягушки, Ниджейма-Шредера, Отвэй-Риса	4
4.	Системы шифрования с открытым ключом.	Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний.	4
5.	Общая схема функционирования систем с открытыми ключами	Цифровые сертификаты и инфраструктура открытых ключей	4
6.	Криптосистема RSA и ее модификации	Цифровые сертификаты и инфраструктура открытых ключей	4
7.	Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля	Тесты на простоту: пробное деление, тест Ферма, тест Миллера-Рабина. Алгоритмы факторизации: пробное деление, гладкие числа, (P-1)-метод Полларда, разность квадратов, современные методы факторизации.	4
8.	Тесты на простоту и факторизация	Виды атак: Атака Винера на RSA, атаки на RSA основанные на решетках, атака Хостада, атака Франклина-Рейтера, частичное раскрытие ключа.	2
Итого по дисциплине			**30**

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Лось А.Б.Криптографические методы защиты информации 2-е изд. Учебник для академического бакалавриата Лось А.Б., Нестеренко А.Ю., Рожков М.И. Изд-во:Научная школа: Национальный исследовательский университет "Высшая школа экономики" (НИУ ВШЭ) (г. Москва). 2016г.-473с.

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 с.

3. Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс]: учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— СПб.: Российский государственный гидрометеорологический университет, 2010.— 104 с

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 указания для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие, включающее:
- конспект лекций;
- методические указания по выполнению лабораторных работ;
- методические указания по выполнению практических (семинарских) работ.

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

Электронное учебное пособие, включающее:
- методические рекомендации для студентов по самостоятельной работе;
- методические рекомендации по выполнению индивидуальных домашних заданий;
- методические рекомендации по выполнению курсовой работы (проекта).

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

1. Secret Disk 4 Lite.
2. InfoWatch CryptoStorage.
3. Rohos Disk.
4. TrueCrypt.
5. WipNet.

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

1. http://fstec.ru/normotvorcheskaya/akty
2. http://ivo.garant.ru/#/startpage:0
3. http://www.consultant.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

Номер ПЗ	Тема практических занятий	Название специализированной лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
1	2	3	4	5
ПЗ-1	Поточные системы шифрования (РСЛОС, RC4, Рона)	Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 460014, Оренбургская область, г. Оренбург, улица Ленинская, , д. 59 учебный корпус 9, каб. №945	Специализированная мебель: учебная доска, стол и стул преподавателя, посадочные места для студентов. Набор демонстрационного оборудования с возможностью использования мультимедиа, экран переносной, ноутбук. Оборудование по защите информации от утечки по акустическому каналу, Демонстрационное специализированное оборудование по защите информации по каналу побочных электромагнитных излучений и наводок Навигатор П-5, аппаратно-программный криптографический	JoliTest (JTRun, JTEditor, TestRun), Свидетельство о государственной регистрации программы для ЭВМ «Система тестирования знаний «JoliTest» от 16.06.2009 № 2009613178 Open Office Лицензия на право использования программного обеспечения Open Office\Apache , Версия 2.0, от января 2004г.
ПЗ-2	Поточные системы шифрования (РСЛОС, RC4, Рона)			
ПЗ-3	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)			
ПЗ-4	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)			
ПЗ-5	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)			
ПЗ-6	Схемы			

	распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)		комплекс для защиты информации КРИПТОН-IDE, измеритель спектра вторичных полей Детектор нелинейных переходов «NR-мю»	
ПЗ-7	Асимметричные криптосистемы (***RSA***, ElGamal, Рабина) Формирование ассиметричных криптосистем			
ПЗ-8	Асимметричные криптосистемы (***RSA***, ElGamal, Рабина) Формирование ассиметричных криптосистем			
ПЗ-9	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)			

Занятия лекционного типа проводятся в учебной аудитории для проведения занятий лекционного типа с набором демонстрационного оборудования, обеспечивающие тематические иллюстрации, укомплектованной специализированной мебелью и техническими средствами обучения.

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.

Программа разработана в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утвержденным приказом Министерства образования и науки РФ № 1509 от 01.12.2016

Разработал(и): _____ Н.П. Мошуров