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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.16 Криптографические методы защиты информации

Направление подготовки 10.03.01 Информационная безопасность

Профиль подготовки Безопасность автоматизированных систем

Квалификация выпускника бакалавр

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	Социология Основы информационной безопасности
ПК-1	Аппаратные средства вычислительной техники
ПК-1	Автоматизированные системы обработки информации
ПК-1	Основы радиотехники

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ОК-5	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)
ПК-1	Производственная (преддипломная) практика
ПК-1	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)

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	Этап 1 Цели, задачи, принципы и основные направления обеспечения криптографической информационно	Этап 1 Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять	Этап 1 Профессиональной терминологией и методами теоретического обоснования в выборе криптографических

деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	й безопасности государства	повышение уровня защиты с учетом криптографических средств защиты информации	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-1 – способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Этап 1: знать принципы построения криптографических алгоритмов	Этап 1: уметь выполнять настройки по обслуживанию криптосистем	Этап 1: выполнения настроек по обслуживанию криптосистем;
ПК-1 – способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Этап 2: знать криптографические стандарты и их использование в информационных системах	Этап 2: уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием криптосистем	Этап 2: осуществления мер противодействия нарушениям сетевой безопасности с использованием криптосистем

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		Семестр №7	
				КР	СР	КР	СР
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Лекции (Л)	50		16		34	
2	Лабораторные работы (ЛР)						
3	Практические занятия (ПЗ)	48		14		34	
4	Семинары(С)						
5	Курсовое проектирование (КП)						
6	Рефераты (Р)						
7	Эссе (Э)						
8	Индивидуальные домашние задания (ИДЗ)						
9	Самостоятельное изучение вопросов (СИВ)		20		10		10
10	Подготовка к занятиям (ПкЗ)		56		30		26
11	Промежуточная аттестация	6		2		4	
12	Наименование вида промежуточной аттестации	x	x	зачет		экзамен	
13	Всего	104	76	32	40	72	36

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		8			x		4	12	x	ПК-1 ОК-5
1.1.	**Тема 1** Классификация криптографических систем	6	4		4			x		2	6	x	ПК-1 ОК-5
1.2.	**Тема 2** Простые шифры и их свойства	6	4		4			x		2	6	x	ПК-1 ОК-5
2.	**Раздел 2 Современные симметричные криптосистемы. Распределение ключей**	6	8		6			x		6	18	x	ПК-1 ОК-5
2.1.	**Тема 3** Симметричные системы шифрования (системы шифрования с секретным	6	4		2			x		2	6	x	ПК-1 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
	ключом)												
2.2.	**Тема 4** Системы шифрования с открытым ключом	6	2		2			x		2	6	x	ПК-1 ОК-5
2.3	**Тема 5** Поточные системы шифрования	6	2		2			x		2	6	x	ПК-1
3.	**Контактная работа**	6	16		14			x				2	x
4.	**Самостоятельная работа**	6						x		10	30		x
5.	**Объем дисциплины в семестре**	6	16		14			x		10	30	2	x
6.	**Раздел 3 Асимметричные криптосистемы**	7	18		18			x		6	14	x	ПК-1 ОК-5
6.1.	**Тема 6** Электронно-цифровая подпись	7	8		8			x		2	8	x	ПК-1
6.2.	**Тема 7** Протоколы идентификации	7	10		10			x		4	6	x	ПК-1
7.	**Раздел 4 Криптографические протоколы**	7	16		16			x		4	12	x	ПК-1 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
7.1.	**Тема 8** Протоколы управления ключами	7	8		8			x		2	6	x	ПК-1
7.2.	**Тема 9** Современные достижения науки и техники в области современной криптографии	7	8		8			x		2	6	x	ПК-1 ОК-5
12.	**Контактная работа**	7	34		34			x				4	x
12.	**Самостоятельная работа**	7						x		10	26		x
14.	**Объем дисциплины в семестре**	7	34		34			x		10	26	4	x
15.	**Всего по дисциплине**	x	50		48			x		20	56	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	Стойкость криптографических систем и алгоритмов	**2**
Л-6	Вычислительные алгоритмы	**2**
Л-7	Блочные и поточные шифры	**2**
Л-8	Блочные и поточные шифры	**2**
Л-9	Шифры DES, режимы работы DES, AES, ГОСТ 28147-89	**2**
Л-10	Шифры DES, режимы работы DES, AES, ГОСТ 28147-89	**2**
Л-11	Поточные шифры: РСЛОС, RC4, шифр Рона	**2**
Л-12	Распределение ключей	**2**
Л-13	Распределение ключей	**2**
Л-14	Общая схема функционирования систем с открытыми ключами	**2**
Л-15	Криптосистема RSA и ее модификации. Криптосистема Эль Гамаля. Криптосистема Рабина	**2**
Л-16	Целостность данных и аутентификация сообщений	**2**
Л-17	Целостность данных и аутентификация сообщений	**2**
Л-18	Хэш-функции	**2**
Л-19	Хэш-функции	**2**
Л-20	Реализация схем электронной цифровой подписи (на основе алгоритмов RSA, ElGamal, Шнорра)	**2**
Л-21	Реализация схем электронной цифровой подписи (на основе алгоритмов RSA, ElGamal, Шнорра)	**2**
Л-22	Криптографические протоколы	**2**
Л-23	Криптографические протоколы	**2**
Л-24	Тесты на простоту и факторизация	**22**
Л-25	Тесты на простоту и факторизация	
Итого по дисциплине		

5.2.2 – 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	Поточные системы шифрования (РСЛОС, RC4, Рона)	**2**
ПЗ-4	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)	**2**
ПЗ-5	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)	**2**
ПЗ-6	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)	**2**
ПЗ-7	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	**2**
ПЗ-8	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	**2**
ПЗ-9	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	**2**
ПЗ-10	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	**2**
ПЗ-11	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	**2**
ПЗ-12	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	**2**
ПЗ-13	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	**2**
ПЗ-14	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	**2**
ПЗ-15	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	**2**
ПЗ-16	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	**2**
ПЗ-17	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	**2**
ПЗ-18	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных	**2**

	криптосистем	
ПЗ-19	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	**2**
ПЗ-20	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	**2**
ПЗ-21	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	**2**
ПЗ-22	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	**2**
ПЗ-23	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	**2**
ПЗ-24	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	**2**
Итого по дисциплине		

5.2.3 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Классификация криптографических систем.	Законодательные и правовые основы защиты компьютерной информации и информационных технологий	2
2.	Простые шифры и их свойства.	Модульная арифметика	2
3.	Симметричные системы шифрования (системы шифрования с секретным ключом).	Схемы обмена секретными ключами: широкоротой лягушки, Ниджейма-Шредера, Отвэй-Риса	2
4.	Системы шифрования с открытым ключом.	Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний.	2
5.	Поточные системы шифрования.	Цифровые сертификаты и инфраструктура открытых ключей	2
6.	Электронно-цифровая подпись.	Цифровые сертификаты и инфраструктура открытых ключей	2
7.	Протоколы идентификации.	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.	Протоколы управления	Виды атак: Атака Винера	2

	ключами.	на RSA, атаки на RSA основанные на решетках, атака Хостада, атака Франклина-Рейтера, частичное раскрытие ключа.	
9.	Современные достижения науки и техники в области современной криптографии.	Стойкость актуальных алгоритмов шифрования. Доказуемая стойкость со случайным оракулом. Доказуемая стойкость без случайного оракула	2
Итого по дисциплине			

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1.Лось А.Б. Криптографические методы защиты информации:учебник для академического бакалавриата/А.Б.Лось, А.Ю. Нестеренко, М.И. Рожков.-2-е изд.испр.-М.; Издательство Юрайт,2016.-473с.

2. Фомичев В.М., Криптографические методы защиты информации в 2 ч. часть 1. математические аспекты. Учебник для академического бакалавриата /Мельников Д.А. Фомичев В.М. М.:Научная школа: Национальный исследовательский ядерный университет "МИФИ" (г. Москва) Финансовый университет при Правительстве Российской Федерации . 2016.-209с.

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 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. 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)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet. .
ПЗ-2	Поточные системы шифрования (РСЛОС, RC4, Рона)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-3	Поточные системы шифрования (РСЛОС, RC4, Рона)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-4	Программная реализация поточных систем шифрования (РСЛОС, RC4,	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.

	Рона)			
ПЗ-5	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-6	Программная реализация поточных систем шифрования (РСЛОС, RC4, Рона)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet. .
ПЗ-7	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-8	Схемы распределения ключей(Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-9	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.

	эллиптических кривых)			
ПЗ-10	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-11	Схемы распределения ключей (Шамира, Диффи-Хеллмана, протоколов основанных на эллиптических кривых)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-12	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-13	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-14	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.

	криптосистем			
ПЗ-15	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-16	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-17	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-18	Асимметричные криптосистемы (RSA, ElGamal, Рабина) Формирование ассиметричных криптосистем	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-19	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-20	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.

ПЗ-21	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-22	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-23	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.
ПЗ-24	Программная реализация асимметричных криптосистем (RSA, ElGamal, Рабина)	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ	1. Secret Disk 4 Lite. 2. InfoWatch CryptoStorage. 3. Rohos Disk. 4. TrueCrypt. 5. WipNet.

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.

Оценочный материал для проведения промежуточной аттестации обучающихся по дисциплине представлен в Приложении 6.

Программа разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденным приказом Министерства образования и науки РФ № 1515 от 01.12.2016 г.

Разработал(и): _____ А.С. Боровский