ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯПРОГРАММАДИСЦИПЛИНЫ

Б1.О.10 МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки (специальность) 10.03.01 Информационная безопасность

Профиль подготовки (специализация) 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

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 Б1.О.10 Методы и средства криптографической защиты информации относится к обязательной части учебного плана. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Методы и средства криптографической защиты информации» является основополагающей, представлен в таблице 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ОПК-9	Производственная технологическая практика
ОПК-4.3	Производственная технологическая практика Производственная эксплуатационная практика

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ОПК-9	Защита информации от утечки по технических каналам

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

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине (модулю)**
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 Применяет математические модели и решать задачи криптографического преобразования при решении задач защиты информации	*Знать:* Основные принципы построения криптоалгоритмов *Уметь:* Строить современные шифрсистемы *Владеть:* Криптографической терминологией

ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.2 Определяет и анализирует технические каналы утечки информации	*Знать:* Каналы утечки информации и методы их оценки *Уметь:* Изучать и анализировать характеристики и особенности применения основных приборов и оборудования, используемых для выявления каналов утечки информации *Владеть:* Расчета контролируемой зоны, в пределах которой могут происходить утечки информации
	ОПК-9.3 Проводит работы по установке и настройке средств технической защиты информации	*Знать:* Понятие составляющие и проблемы информационной безопасности *Уметь:* Обосновать и сформулировать решения по применению технологических и нормативно-правовых средств и методов Обеспечения информационной безопасности *Владеть:* Методом дискретного логарифмирования в конечных циклических группах
ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;	ОПК-4.3.1 Способен применять основные угрозы компьютерной информации, реализуемые на различных уровнях программной иерархии и типы атак	*Знать:* Объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные и аппаратные средства *Уметь:* Применять криптографические и информационно-аналитические системы, информационные ресурсы и информационные технологии *Владеть:* Методом применения основных криптосистем и систем стенографирования

ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;	ОПК-4.3.2 Выявляет принципы построения подсистем защиты компьютерной информации в операционных системах и в пользовательских программных приложениях	*Знать:* Основные принципы построения подсистем защиты компьютерной информации и в операционных системах и в пользовательских программных приложениях *Уметь:* Планировать программно-аппаратную подсистему политики безопасности организации *Владеть:* Методами защиты информации в операционных системах и в пользовательских приложениях
	ОПК-4.3.3 Способен использовать сертифицированные и перспективные программно-аппаратные средства и методы защиты компьютерной информации (в том числе криптографических)	*Знать:* Виды информации, подлежащей шифрованию *Уметь:* Применять частотные характеристики языков и их использование в криптоанализе *Владеть:* Методами криптоанализа простейших шифров
	ОПК-4.3.4 Выявляет средства и методы защиты от НСД хранимой информации с использованием возможностей устройств	*Знать:* Средства и методы защиты от НСД хранимой информации с использованием возможностей устройств записи и чтения *Уметь:* Использовать криптографические методы при организации работ по защите информации *Владеть:* Навыками использования инструментов криптографической защиты информации

4. Объем дисциплины

Объем дисциплины Б1.О.10 Методы и средства криптографической защиты информации составляет 5 зачетных(ые) единиц(ы) (ЗЕ), (180 академических часов), распределение объёма 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

Вид учебной работы	Итого КР	Итого СР	Семестр №6		Семестр №7	
			КР	С	КР	СР
Лекции (Л)	36		18		18	
Лабораторные работы (ЛР)						
Практические занятия (ПЗ)	50		16		34	
Семинары(С)						
Курсовое проектирование (КП)						
Самостоятельная работа		88		36		52
Промежуточная аттестация	6		2		4	
Наименование вида промежуточной аттестации	x	x	Зачёт		Экзамен	
Всего	92	88	36	36	56	52

5. Структура и содержание дисциплины

Структура и содержание дисциплины представлены в таблице 5.1.

Таблица 5.1 – Структура и содержание дисциплины

Наименование тем	Семестр	Объем работы по видам учебных занятий, академические часы									Коды формируемых компетенций, код индикатора достижения компетенции
		лекции	Лабораторная работа	Практические занятия	семинары	Курсовое проектирование	индивидуальныеидомашние задания (контрольные работы)	Самостоятельноеизучениев опросов	подготовка к занятиям	Промежуточнаяаттестация	
Тема 1. Классификацияк риптографическихсистем	6	2		2				6			ОПК-4.3.1, ОПК -9.3, ОПК-4.3.2, ОПК-4.3.3

Тема 2. Простые шифры и их свойства	6	4		4				6			ОПК-9.1, ОПК-9.2, ОПК-9.3, ОПК-4.3.1
Тема 3. Симметричные системы шифрования (системы шифрования с секретным ключом)	6	4		4				10			ОПК-4.3.3, ОПК-4.3.4, ОПК-9.2, ОПК-4.3.2
Тема 4. Системы шифрования с открытым ключом	6	4		4				6			ОПК-4.3.1, ОПК-4.3.2, ОПК-4.3.3, ОПК-9.1, ОПК-9.3
Тема 5. Поточные системы шифрования	6	4		2				8			ОПК-9.1, ОПК-4.3.3, ОПК-4.3.4, ОПК-9.2
Контактная работа	6	18		16						2	x
Самостоятельная работа	6							36			x
Объем дисциплины в семестре	6	18		16				36		2	x
Тема 6. Электронно-цифровая подпись	7	4		8				12			ОПК-4.3.1, ОПК-4.3.2, ОПК-4.3.3
Тема 7. Протоколы идентификации	7	4		8				12			ОПК-4.3.1, ОПК-4.3.2, ОПК-4.3.3
Тема 8. Протоколы управления ключами	7	4		8				14			ОПК-4.3.4, ОПК-9.2, ОПК-9.3
Тема 9. Современные достижения науки и техники в области современной криптографии	7	6		10				14			ОПК-4.3.2, ОПК-4.3.3, ОПК-9.1, ОПК-9.3
Контактная работа	7	18		34						4	x
Самостоятельная работа	7							52			x
Объем дисциплины в семестре	7	18		34				52		4	x
Всего по дисциплине		36		50				88		6	

5.2. Темы курсовых работ (проектов)
Не предусмотрены

5.3. Темы индивидуальных домашних заданий (контрольных работ)
Не предусмотрены

5.4 Вопросы для самостоятельного изученияпо очной форме обучения

№ п.п.	Наименования темы	Наименование вопросов	Объем, академические часы
1	Классификация криптографических систем	Выявить основную классификацию криптографических систем	6
2	Простые шифры и их свойства	Рассмотреть простые шифры и их свойства	6
3	Симметричные системы шифрования (системы шифрования с секретным ключом)	Раскрыть основные симметричные системы шифрования (системы шифрования с секретным ключом)	10
4	Системы шифрования с открытым ключом	Рассмотреть системы шифрования с открытым ключом	6
5	Поточные системы шифрования	Рассмотреть поточные системы шифрования	8
6	Электронно-цифровая подпись	Рассмотреть электронно- цифровая подпись	12
7	Протоколы идентификации	Рассмотреть протоколы идентификации	12
8	Протоколы управления ключами	Рассмотреть протоколы управления ключами	14
9	Современные достижения науки и техники в области современной криптографии	Рассмотреть современные достижения науки и техники в области современной криптографии	14
		Всего	88

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1.Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система.

2. Математическая логика и теория алгоритмов : учебное пособие / составители А. Н. Макоха. — Ставрополь : СКФУ, 2017. — 418 с. — Текст : электронный // Лань : электронно-библиотечная система.

3. Овчинников, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Овчинников. — Санкт-Петербург : ГУАП, 2021. — 133 с. — ISBN 978-5-8088-1591-9. — Текст : электронный // Лань : электронно-библиотечная система.

4. Жуков, А. Е. Системы блочного шифрования : учебное пособие / А. Е. Жуков. — Москва : МГТУ им. Н.Э. Баумана, 2013. — 77 с. — ISBN 978-5-7038-3753-5. — Текст : электронный // Лань : электронно-библиотечная система.

5. Бурова, М. А. Информационная безопасность и защита информации : учебное пособие / М. А. Бурова, А. С. Овсянников. — Самара : СамГУПС, [б. г.]. — Часть 2 — 2012. — 150 с. — Текст : электронный // Лань : электронно-библиотечная система.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1.Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система.

2.Рацеев, С. М. Математические методы защиты информации : учебное пособие для вузов / С. М. Рацеев. — Санкт-Петербург : Лань, 2022. — 544 с. — ISBN 978-5-8114-8589-5. — Текст : электронный // Лань : электронно-библиотечная система.

3.Титовская, Н. В. Информационные технологии обеспечения конфиденциальности и сохранности данных : учебное пособие / Н. В. Титовская, С. Н. Титовский. — Красноярск : КрасГАУ, 2018. — 178 с. — Текст : электронный // Лань : электронно-библиотечная система.

4. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система.

6.3 Методические материалы для обучающихся по освоению дисциплины

Тематическое содержание дисциплины

7. Требования к материально-техническому и учебно-методическому содержанию дисциплины

7.1 Учебные аудитории для проведения учебных занятий по дисциплине

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, укомплектованных специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

7.2 Перечень оборудования и технических средств обучения по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиа -проектором, компьютером и учебной доской.

7.3 Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. JoliTest (JTRun, JTEditor, TestRun)
2. MS Office

7.4 Современные профессиональные базы данных и информационно-справочные системы

1. Консультант +.

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

Программа разработана в соответствии с Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

Разработал(и):

Заведующий кафедрой,к.т.н. _____ Урбан Владимир Александрович

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 19.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович

Программа рассмотрена и утверждена на заседании Ученого совета Института управления рисками и комплексной безопасности, протокол № 4 от 22.02.2021 г.

Директор Института управления рисками и комплексной безопасности

_____ Яковлева Евгения Васильевна

Дополнения и изменения

в рабочей программе дисциплины Б1.О.10 Методы и средства криптографической защиты информации на 2021 - 2022 учебный год.

В программу вносятся следующие изменения: без изменений

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович