

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Клочков Юрий Сергеевич
Должность: и.о. ректора
Дата подписания: 03.04.2024 09:42:14
Уникальный программный ключ:
4e7c4ea90328ec8e65c5d8058549a2538d7400d1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТОМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Руководитель образовательной
программы

_____ У.В. Лаптева
« _____ » _____ 2023 г.

РАБОЧАЯ ПРОГРАММА

дисциплины: **Методы криптографии**

направление подготовки: **09.03.02 Информационные системы и технологии**

направленность (профиль): **Искусственный интеллект и программирование**

форма обучения: **очная**

Рабочая программа рассмотрена
на заседании кафедры Интеллектуальных систем и технологий

Протокол № ___ от _____ 20__ г.

1. Цели и задачи освоения дисциплины

Целью изучения дисциплины является овладение обучающимися основными знаниями, связанными с защитой информации путем математических преобразований с помощью криптографических алгоритмов.

Задачи дисциплины

- изучение основных математических подходов к решению задач компьютерной безопасности;
- обучить применению программных и аппаратных средств, реализующих основные криптографические функции.

Обучающиеся должны знать основные задачи и понятия криптографии, требования к шифрам и основные характеристики шифров, принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к части учебного плана, формируемой участниками образовательных отношений.

Необходимыми условиями для освоения дисциплины являются:

Знания, полученные при изучении математических, естественнонаучных дисциплин, информационных технологий и программирования.

Умение анализировать предметную область, выделять проблему и формулировать решение.

Владение методиками использования программных средств для решения практических задач.

Содержание дисциплины является логическим продолжением содержания дисциплин математической, компьютерно - информационной и научно-исследовательской направленности, может быть использовано для подготовки и написания ВКР.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине
ПКС-6 Способен анализировать большие данные с использованием существующей методологической и технологической инфраструктуры	ПКС-6.1 Подготавливает данные для проведения аналитических работ и проводит аналитические исследования в том числе с применением технологий больших данных	Знать: 31 - математические основы современной криптографии; модели шифров и математические методы их исследования. 32 - место криптографии в задаче информационной безопасности и построения защищенных информационных систем
		Уметь: У1 – применять математические методы криптографической защиты информации У2 - ориентироваться в современной системе источников информации; видеть и формулировать проблему защиты информации; Использовать криптографические методы при организации работ по защите информации
		Владеть: В1 - навыками математического моделирования в криптографии В2 - навыками самостоятельной исследовательской работы
ПКС-9 Способен	ПКС-9.2	Знать:

проводить научно-исследовательские работы, выполнять построение моделей и постановку вычислительных экспериментов как в целом по теме проекта, так и по отдельным разделам	Проводит эксперименты, наблюдения и измерения в области систем искусственного интеллекта, обобщает результаты; разрабатывает модели, строит оптимальные системы на основе исследовательских результатов	33 - основные задачи и понятия криптографии 34 - основные задачи и понятия криптографии 35 - требования к шифрам и основные характеристики шифров 36 - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах
		Уметь: У3 - использовать программные и аппаратные средства персонального компьютера; пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа У4 - выполнять шифрование и дешифрование текста с помощью различных криптоалгоритмов, осуществлять программирование используемых алгоритмов, проводить строгую математическую проверку стойкости шифра
		Владеть: В3 - навыками использования инструментов криптографической защиты информации В4 - способами построения типовых криптографических алгоритмов

4. Объем дисциплины

Общий объем дисциплины составляет 3 зачетных единиц, 108 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	3/5	18	18	18	27	27	Экзамен

5. Структура и содержание дисциплины

5.1. Структура дисциплины

очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Простые шифры	4	-	-	6	10	ПКС-6.1 ПКС-9.2	Опрос
2	2	Шифрование с закрытым ключом	4	4	4	7	19	ПКС-6.1 ПКС-9.2	Опрос, Отчёт по лабораторным работам

3	3	Блочные шифры	5	9	9	7	30	ПКС-6.1 ПКС-9.2	Опрос, Отчёт по лабораторн ым работам
4	4	Шифрование с открытым ключом	5	5	5	7	22	ПКС-6.1 ПКС-9.2	Опрос, Отчёт по лабораторн ым работам
5	Экзамен		-	-	-	-	27	ПКС-6.1 ПКС-9.2	Письменн ый опрос
Итого:			18	18	18	27	108		

заочная форма обучения (ЗФО): не реализуется

очно-заочная форма обучения (ОЗФО): не реализуется

5.2. Содержание дисциплины

5.2.1. Содержание разделов дисциплины

Раздел 1. «*Простые шифры*». Основные понятия криптографии. Введение в криптографию. Криптографические атаки. Криптографический протокол. Шифр Цезаря. Методы простой замены. Шифр Виженера. Частотный анализ.

Раздел 2. «*Шифрование с закрытым ключом*». Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ. Шифры гаммирования. Понятие композиционного шифра. Композиции шифров.

Раздел 3. «*Блочные шифры*». Алгоритмы шифрования DES и AES. Хеширование. Принципы построения блочных шифров с закрытым ключом. Режимы работы блочных шифров. Сеть Фейштеля. Алгоритмы шифрования DES и AES. Общие сведения. Шифрование и расшифрование. Криптографические хеш-функции. Понятие хеш-функции. Обзор алгоритмов формирования хеш-функций.

Раздел 4. «*Шифрование с открытым ключом*». Шифры с открытым ключом. Алгоритм RSA. Электронная цифровая подпись. Криптостойкость и имитостойкость шифров. Шифры с открытым ключом. Односторонние функции. Использование ассиметричных алгоритмов для шифрования. Алгоритм RSA. Основные сведения. Пример вычислений по алгоритму. Практическое использование алгоритма RSA. Электронная цифровая подпись Криптостойкость и имитостойкость шифров.

5.2.2. Содержание дисциплины по видам учебных занятий.

Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лекции
		ОФО	ЗФО	ОЗФО	
1	1	4	-	-	Введение криптографию Шифр Цезаря. Шифр простой замены Шифр Виженера. Частотный анализ.
2	2	4	-	-	Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ Шифры гаммирования. Композиции шифров

3	3	5	-	-	Сеть Фейстеля DES/3DES AES
4	4	5	-	-	Алгоритм Хелмана RSA
Итого:		18	-	-	

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Наименование лабораторной работы
		ОФО	ЗФО	ОЗФО	
1	2	4	-	-	Шифр Цезаря. Шифр простой замены
2	3	4	-	-	Шифры гаммирования.
3	3	5	-	-	Сеть Фейстеля
4	4	5	-	-	Алгоритм Хелмана
Итого:		18	-	-	

Практические занятия

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Наименование лабораторной работы
		ОФО	ЗФО	ОЗФО	
1	2	4	-	-	Шифр Виженера. Частотный анализ.
2	3	4	-	-	Композиции шифров
3	3	5	-	-	DES/3DES AES
4	4	5	-	-	RSA
Итого:		18	-	-	

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОЗФО		
1	1	6	--	-	Изучение функций библиотек GNU MP и GNU Сcrypto по технической документации	Подготовка к защите темы дисциплины (собеседование) Подготовка к лабораторным работам, оформление отчетов к лабораторным работам
2	2	7	-	-	Инструментальные средства и библиотеки для реализации криптографических алгоритмов	Подготовка к защите темы дисциплины (собеседование) Подготовка к лабораторным работам, оформление отчетов к лабораторным работам
3	3	7	-	-	Теоретико –числовые методы в криптографии. Вычисления в простых полях и кольцах целых чисел	Подготовка к защите темы дисциплины (собеседование) Подготовка к лабораторным работам, оформление отчетов к лабораторным работам

4	4	7	-	-	Система Диффи-Хеллмана, шифр Шамира, шифр Эль - Гамалья	Подготовка к защите темы дисциплины (собеседование) Подготовка к лабораторным работам, оформление отчетов к лабораторным работам
Итого:		27		-		

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий: практико-модульное, проектно-ориентированное обучение и смешанных (обучение с использованием системы blendedlearning - используются специальные информационные технологии, такие как компьютерная графика, аудио и видео, интерактивные элементы и т.п), обучение в дистанционном формате.

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены

7. Контрольные работы для заочной формы обучения

Заочная форма не реализуется

8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1.

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1 текущая аттестация		
1	Выполнение и защита лабораторных работ №1	0-10
2	Собеседование по Разделу 1	0-20
	ИТОГО за первую текущую аттестацию	30
2 текущая аттестация		
3	Выполнение и защита лабораторных работ №2-3	0-20
4	Собеседование по Разделам 2, 3 дисциплины	0-20
	ИТОГО за вторую текущую аттестацию	40
3 текущая аттестация		
5	Выполнение и защита лабораторных работ №4	0-10
6	Собеседование по Разделу 4 дисциплины	0-20
	ИТОГО за третью текущую аттестацию	30
	ВСЕГО	100

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы

1 Сайт ФГБОУВО ТИУ - <http://www.tyuiu.ru/>

- 2 Система поддержки дистанционного обучения Educon - <http://educon2.tyuiu.ru/>
- 3 Электронный каталог Библиотечно-издательского комплекса -<http://webirbis.tsogu.ru/>
- 4 Электронная библиотечная система eLib -<http://elib.tsogu.ru/>
- 5 Научная электронная библиотека eLibrary.ru -<http://elibrary.ru/defaultx.asp>
- 6 ЭБС издательства «Лань» - <http://e.lanbook.com>
- 7 Официальный сайт компании «Консультант Плюс» - <http://www.consultant.ru>
- 8 Международная Электротехническая Комиссия МЭК - <http://www.iec.ch>
- 9 Международная Организация по Стандартизации ISO - <http://www.iso.org/iso.ru>
- 10 Единый портал тестирования в сфере образования - <http://www.i-exam.ru>
- 11 Открытая программная библиотека для машинного обучения для решения задач построения и тренировки нейронной сети с целью автоматического нахождения и классификации образов, достигая качества человеческого восприятия [TensorFlow](#)
- 12 Фреймворк машинного обучения для языка Python с открытым исходным кодом, созданный на базе [PyTorch](#)
- 13 Открытая библиотека, написанная на языке Python и обеспечивающая взаимодействие с искусственными нейронными сетями [KERAS](#)

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства

- 1 Python;
- 2 C++;
- 3 MathCAD, Mat Lab и др.
- 4 Visual Studio Community (свободно-распространяемое ПО)
- 5 Microsoft Windows;
- 6 Microsoft Office Professional Plus;

10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

Обеспеченность материально-технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
1	Методы криптографии	<p>Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Учебная мебель: столы, стулья, доска аудиторная. Моноблок - 1 шт., проектор - 1 шт., акустическая система (колонки) - 4 шт., проекционный экран - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.</p> <p>Лабораторные занятия: Учебная аудитория для проведения занятий семинарского типа (практические занятия);</p>	<p>625039, Тюменская область, г. Тюмень, ул. Мельникайте, д. 70</p> <p>625039, Тюменская область, г. Тюмень, ул. Мельникайте, д. 70</p>

		групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации, Учебная мебель: столы, стулья, доска аудиторная. Моноблок - 1 шт., проектор - 1 шт., акустическая система (колонки) - 4 шт., проекционный экран - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	
--	--	---	--

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим, лабораторным занятиям. Лабораторные работы по данной дисциплине не предусмотрены учебным планом.

При подготовке к практическим занятиям обучающемуся рекомендуется повторить теоретический лекционный материал, а также прочитать соответствующие темы в основной и дополнительной рекомендуемой литературе. Составить перечень возникших в ходе изучения материала вопросов и обсудить возникшие вопросы с преподавателем до начала выполнения лабораторной работы.

11.2 Методические указания по организации самостоятельной работы.

Самостоятельная работа обучающихся заключается в получении заданий (тем) у преподавателя для индивидуального освоения. Преподаватель на занятии дает рекомендации, необходимые для освоения материала. В ходе самостоятельной работы обучающиеся должны выполнить задания на компьютере с помощью пакетов прикладных программ, изучить теоретический материал по разделам. Обучающиеся должны понимать содержание выполненной работы (знать определения понятий, уметь разъяснить значение и смысл любого термина, используемого в работе и т.п). Более подробно порядок выполнения заданий изложен в следующих методических указаниях:

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: Методы криптографии

Код, направление подготовки: **09.03.02 Информационные системы и технологии**

Направленность (профиль): **Искусственный интеллект и программирование**

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-6 Способен анализировать большие данные с использованием существующей методологической и технологической инфраструктуры	ПКС-6.1 Подготавливает данные для проведения аналитических работ и проводит аналитические исследования в том числе с применением технологий больших данных	Знать: 31 - математические основы современной криптографии; модели шифров и математические методы их исследования. 32 - место криптографии в задаче информационной безопасности и построения защищенных информационных систем	Не знает - математические основы современной криптографии; модели шифров и математические методы их исследования. - место криптографии в задаче информационной безопасности и построения защищенных информационных систем	Знает частично - математические основы современной криптографии; модели шифров и математические методы их исследования. - место криптографии в задаче информационной безопасности и построения защищенных информационных систем	Знает - математические основы современной криптографии; модели шифров и математические методы их исследования. - место криптографии в задаче информационной безопасности и построения защищенных информационных систем	Отлично знает - математические основы современной криптографии; модели шифров и математические методы их исследования. - место криптографии в задаче информационной безопасности и построения защищенных информационных систем
		Уметь: У1 – применять математические методы криптографической защиты информации У2 - ориентироваться в современной системе источников информации; видеть и формулировать проблему защиты информации;	Не умеет – применять математические методы криптографической защиты информации - ориентироваться в современной системе источников информации; видеть	Умеет частично – применять математические методы криптографической защиты информации - ориентироваться в современной системе источников информации; видеть	Умеет – применять математические методы криптографической защиты информации - ориентироваться в современной системе источников информации; видеть	Уверенно умеет – применять математические методы криптографической защиты информации - ориентироваться в современной системе источников информации; видеть

		Использовать криптографические методы при организации работ по защите информации	и формулировать проблему защиты информации; Использовать криптографические методы при организации работ по защите информации	и формулировать проблему защиты информации; Использовать криптографические методы при организации работ по защите информации	и формулировать проблему защиты информации; Использовать криптографические методы при организации работ по защите информации	и формулировать проблему защиты информации; Использовать криптографические методы при организации работ по защите информации
		Владеть: В1 - навыками математического моделирования в криптографии В2 - навыками самостоятельной исследовательской работы	Не владеет - навыками математического моделирования в криптографии - навыками самостоятельной исследовательской работы	Плохо владеет - навыками математического моделирования в криптографии - навыками самостоятельной исследовательской работы	Владеет - навыками математического моделирования в криптографии - навыками самостоятельной исследовательской работы	Прекрасно владеет - навыками математического моделирования в криптографии - навыками самостоятельной исследовательской работы
ПКС-9 Способен проводить научно-исследовательские работы, выполнять построение моделей и постановку вычислительных экспериментов как в целом по теме проекта, так и по отдельным разделам	ПКС-9.2 Проводит эксперименты, наблюдения и измерения в области систем искусственного интеллекта, обобщает результаты; разрабатывает модели, строит оптимальные системы на основе исследовательских результатов	Знать: 33 - основные задачи и понятия криптографии 34 - основные задачи и понятия криптографии 35 - требования к шифрам и основные характеристики шифров 36 - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах	Не знает - основные задачи и понятия криптографии - основные задачи и понятия криптографии - требования к шифрам и основные характеристики шифров - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах	Знает частично - основные задачи и понятия криптографии - основные задачи и понятия криптографии - требования к шифрам и основные характеристики шифров - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах	Знает - основные задачи и понятия криптографии - основные задачи и понятия криптографии - требования к шифрам и основные характеристики шифров - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах	Отлично знает - основные задачи и понятия криптографии - основные задачи и понятия криптографии - требования к шифрам и основные характеристики шифров - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах
		Уметь: У3 - использовать программные и	Не умеет - использовать программные и	Умеет частично - использовать программные и	Умеет - использовать программные и	Уверенно умеет - использовать программные и

		<p>аппаратные средства персонального компьютера; пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа</p> <p>У4 - выполнять шифрование и дешифрование текста с помощью различных криптоалгоритмов, осуществлять программирование используемых алгоритмов, проводить строгую математическую проверку стойкости шифра</p>	<p>аппаратные средства персонального компьютера; пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа</p> <p>- выполнять шифрование и дешифрование текста с помощью различных криптоалгоритмов, осуществлять программирование используемых алгоритмов, проводить строгую математическую проверку стойкости шифра</p>	<p>аппаратные средства персонального компьютера; пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа</p> <p>- выполнять шифрование и дешифрование текста с помощью различных криптоалгоритмов, осуществлять программирование используемых алгоритмов, проводить строгую математическую проверку стойкости шифра</p>	<p>аппаратные средства персонального компьютера; пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа</p> <p>- выполнять шифрование и дешифрование текста с помощью различных криптоалгоритмов, осуществлять программирование используемых алгоритмов, проводить строгую математическую проверку стойкости шифра</p>	<p>аппаратные средства персонального компьютера; пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа</p> <p>- выполнять шифрование и дешифрование текста с помощью различных криптоалгоритмов, осуществлять программирование используемых алгоритмов, проводить строгую математическую проверку стойкости шифра</p>
		<p>Владеть:</p> <p>В3 - навыками использования инструментов криптографической защиты информации</p> <p>В4 - способами построения типовых криптографических алгоритмов</p>	<p>Не владеет</p> <p>- навыками использования инструментов криптографической защиты информации</p> <p>- способами построения типовых криптографических алгоритмов</p>	<p>Плохо владеет</p> <p>- навыками использования инструментов криптографической защиты информации</p> <p>- способами построения типовых криптографических алгоритмов</p>	<p>Владеет</p> <p>- навыками использования инструментов криптографической защиты информации</p> <p>- способами построения типовых криптографических алгоритмов</p>	<p>Прекрасно владеет</p> <p>- навыками использования инструментов криптографической защиты информации</p> <p>- способами построения типовых криптографических алгоритмов</p>

КАРТА
обеспеченности дисциплины (модуля) учебной и учебно-методической литературой

Дисциплина: Методы криптографии

Код, направление подготовки: **09.03.02 Информационные системы и технологии**Направленность (профиль): **Искусственный интеллект и программирование**

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2022. — 400 с. — ISBN 978-5-8114-1116-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/210746 . — Режим доступа: для авториз. пользователей.	ЭР	30	100	+
2	Ильин, М. Е. Теоретико-числовые методы в криптографии : учебное пособие / М. Е. Ильин, К. А. Ципоркова. — Рязань : РГРТУ, 2021 — Часть 2 — 2021. — 80 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/220439 . — Режим доступа: для авториз. пользователей.	ЭР	30	100	+
3	Ильин, М. Е. Теоретико-числовые методы в криптографии : учебное пособие / М. Е. Ильин, К. А. Ципоркова. — Рязань : РГРТУ, 2020 — Часть 1 — 2020. — 112 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168360 . — Режим доступа: для авториз. пользователей.	ЭР	30	100	+
4	Рацеев, С. М. Теоретико-числовые методы в криптографии : учебное пособие / С. М. Рацеев. — Ульяновск : УлГУ, 2020 — Часть 1 — 2020. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/199673 . — Режим доступа: для авториз. пользователей.	ЭР	30	100	+
5	Борисова, С. Н. Криптографические методы защиты информации: классическая криптография : учебное пособие / С. Н. Борисова. — Пенза : ПГУ, 2018. — 186 с. — ISBN 978-5-907102-51-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/162235 . — Режим доступа: для авториз. пользователей.	ЭР	30	100	+

ЭР – электронный ресурс для автор. пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ <http://webirbis.tsogu.ru/>

Лист согласования

Внутренний документ "Методы криптографии_2023_09.03.02_ИСТ (ИИПБ)"

Ответственный: Тутубалина Оксана Викторовна

Дата начала: Дата окончания:

Согласовано

Серийный номер ЭП	Должность	ФИО	ИО	Виза	Комментарий	Дата
	Доцент, не имеющий ученой степени (базовый уровень)	Сидоров Андрей Юрьевич		Согласовано		
	Специалист 1 категории		Радичко Диана Викторовна	Согласовано		
	Директор	Каюкова Дарья Хрисановна	Кислицина Мухаббат Абдурахмановна	Согласовано		