Министерство науки и высшего образования Российской Федерации

Мытищинский филиал

федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)»

(МФ МГТУ им. Н.Э. Баумана)

Заместитель директора
по учебной работе
МФ МГТУ им. Н.Э. Баумана
_____ Макуев В.А.
«25» июня 2021 г.

Факультет К «Космический факультет»

Кафедра К3 «Прикладная математика, информатика и вычислительная техника»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

Автор программы:
Ветошкин А.М., доцент (к.н.), кандидат технических наук, доцент, vetoshkin@bmstu.ru

Утверждена на заседании кафедры «Прикладная математика, информатика и вычислительная техника»
Протокол № 11 заседания кафедры «КЗ» от 18.06.2021 г.

Начальник Отдела образовательных программ
Шевлякова А.А

Рабочая программа одобрена на 2022/2023 учебный год.
Протокол № 9 заседания кафедры «КЗ» от 15.04.2022 г.
Лист переутверждения рабочей программы дисциплины / практики.

Рабочая программа одобрена на 2023/2024 учебный год.
Протокол № 9 заседания кафедры «КЗ» от 14.04.2023 г.
Лист переутверждения рабочей программы дисциплины / практики.

Рабочая программа одобрена на 2024/2025 учебный год.
Протокол № 9 заседания кафедры «КЗ» от 18.04.2024 г.
Лист переутверждения рабочей программы дисциплины / практики.

ОГЛАВЛЕНИЕ

с.

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Настоящая рабочая программа дисциплины устанавливает требования к знаниям и умениям студента, а также определяет содержание и виды учебных занятий и отчетности.

Программа разработана в соответствии с:

• Самостоятельно устанавливаемым образовательным стандартом (СУОС 3++) по направлению подготовки (уровень бакалавриата):09.03.01 «Информатика и вычислительная техника»;

• Основной профессиональной образовательной программой по направлению подготовки 09.03.01 «Информатика и вычислительная техника»;

• Учебным планом МГТУ им. Н.Э. Баумана по направлению подготовки 09.03.01 «Информатика и вычислительная техника».

При освоении дисциплины планируется формирование компетенций, предусмотренных ОПОП на основе СУОС 3++ по направлению подготовки 09.03.01 «Информатика и вычислительная техника» (уровень бакалавриата)

Код компетенции по СУОС 3++	**Формулировка компетенции**
	Общепрофессиональные компетенции собственные
ОПКС-3 (09.03.01)	Способен решать стандартные задачи профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПКС-9 (09.03.01)	Способен осваивать отечественные и зарубежные методики использования программных средств для решения практических задач

Для категорий «знать, уметь, владеть» планируется достижение результатов обучения (РО), вносящих на соответствующих уровнях вклад в формирование компетенций, предусмотренных основной профессиональной образовательной программой (табл. 1).

Таблица 1. Индикаторы достижения компетенции

1	2	3
Компетенция: код по СУОС 3++, формулировка	**Индикаторы**	**Формы и методы обучения, способствующие формированию и развитию компетенции**
ОПКС-3 (09.03.01) Способен решать стандартные задачи профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ЗНАТЬ - основные правила обеспечения информационной безопасности УМЕТЬ - решать стандартные задачи профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ВЛАДЕТЬ - методиками решения стандартных задач профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Лекции** **Лабораторные работы** **Самостоятельная работа** **Активные и интерактивные формы (методы) обучения:** обсуждение практических примеров на лекциях
ОПКС-9 (09.03.01) Способен осваивать отечественные и зарубежные методики использования программных средств для решения практических задач	ЗНАТЬ - подходы к использованию программных средств для решения практических задач УМЕТЬ - осваивать отечественные и зарубежные методики использования программных средств для решения практических задач	**Лекции** **Лабораторные работы** **Самостоятельная работа** **Активные и интерактивные формы (методы) обучения:** обсуждение практических примеров на лекциях

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в блок Б1 «Дисциплины (модули)» образовательной программы бакалавриата по направлению 09.03.01 «Информатика и вычислительная техника».

Изучение дисциплины предполагает предварительное освоение следующих дисциплин учебного плана:

- Математический анализ;
- Дискретная математика;
- Алгебра и геометрия.

Освоение данной дисциплины необходимо как предшествующее для следующих дисциплин образовательной программы:

- Подготовка и защита выпускной квалификационной работы.

Освоение учебной дисциплины связано с формированием компетенций с учетом матрицы компетенций ОПОП для направления (уровень бакалавриата): 09.03.01 Информатика и вычислительная техника .

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общий объем дисциплины составляет 4 зачетные единицы(з.е.), 144 академических часа (108 астрономических часов). В том числе:
1 семестр – 4 з.е. (144 ак.ч.).

Таблица 2. Объём дисциплины по видам учебных занятий (в академических часах)

Виды учебной работы	**Объем по семестрам, акад. ч.**	
	Всего	**Количество семестров освоения дисциплины**
		1
Объем дисциплины	144	144
Аудиторная работа*	**60**	**60**
Лекции (Л)	40	40
Лабораторные работы (ЛР)	20	20
Самостоятельная работа (СР)	**84**	**84**
Проработка учебного материала лекций	5	5
Подготовка к лабораторным работам	10	10
Подготовка к экзамену	30	30
Подготовка к рубежному контролю	6	6
Другие виды самостоятельной работы	33	33
Вид промежуточной аттестации		**Экзамен**

*в том числе, в форме практической подготовки

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО МОДУЛЯМ УЧЕБНОЙ ДИСЦИПЛИНЫ С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ИЛИ АСТРОНОМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Таблица 3. Содержание дисциплины

№ п/п	Тема (название) модуля	Виды занятий*, часы				Активные и интерактивные формы проведения занятий		Компетенции, закрепленные за темой (код по СУОС 3++)	Текущий контроль результатов обучения		
		Л	С	ЛР	СР	Форма проведения занятий	Часы		Срок (неделя)	Формы	Баллы (мин/ макс)
1 семестр											
1	Теория чисел. Криптография.	20	0	12	27	обсуждение практических примеров на лекциях	12	ОПКС-3, ОПКС-9	6	Лабораторные работы	9/15
										Рубежный контроль	12/20
										ИТОГО:	**21/35**
2	Шифрование с открытым ключом. Целочисленная арифметика многократной точности.	20	0	8	27	обсуждение практических примеров на лекциях	8	ОПКС-3, ОПКС-9	12	Лабораторные работы	6/10
										Рубежный контроль	15/25
										ИТОГО:	**21/35**
3	Экзамен	-	-	-	30	-	-	-	-	-	**18/30**
	ИТОГО за семестр	**40**	**0**	**20**	**84**	**-**	**?**	**-**	**-**	**-**	**60/100**

*в том числе, в форме практической подготовки

Содержание дисциплины, структурированное по темам (модулям)

№, п/п	Наименование модуля, содержание	Часы
1	**Теория чисел. Криптография.**	
	Лекции	20
1.1	Сравнения; НОД; алгоритм Евклида; непрерывная дробь; подходящие дроби.	2
1.2	Нахождение обратной величины по модулю; функция Эйлера.	2
1.3	Теорема Эйлера; теорема Ферма; символ Лежандра.	2
1.4	Алгебра; группа, порядок группы; подгруппа; циклическая группа; теорема Лагранжа.	2
1.5	Кольца; примеры колец; кольцо Zm, делители нуля.	2
1.6	Поля; примеры полей; поле Галуа GF(q); мультипликативная группа поля Галуа; примитивный элемент, расширения полей, подполя, характеристика поля.	2
1.7	Криптография; исторические примеры шифров.	2
1.8	Стойкость шифров; абсолютно стойкий шифр; проблема распространения ключей; шифр Цезаря.	2
1.9	Аффинное преобразование; биграммы; шифры подстановки; шифры перестановки.	2
1.10	Потоковые шифры; блочные шифры; симметрические шифросистемы; стандарты шифрования: DES, AES, ГОСТ-28147-89.	2
	Лабораторные работы	12
ЛР1.1	Вычисление вычетов по модулю. Возведение в степень.	4
ЛР1.2	Нахождение обратной величины по модулю, примитивный корень.	4
ЛР1.3	Схема Диффи-Хеллмана.	4
	Самостоятельная работа	27
СР1.1	Проработка учебного материала лекций	2.5
СР1.2	Подготовка к лабораторным работам	6
СР1.3	Подготовка к рубежному контролю	3
СР1.4	Другие виды самостоятельной работы	15.5
2	**Шифрование с открытым ключом. Целочисленная арифметика многократной точности.**	
	Лекции	20
2.1	Шифрование с открытым ключом.	2
2.2	Алгоритм шифрования RSA.	2
2.3	Задачи, трудные для решения – вычисление дискретного логарифма, разложение на множители большого числа.	2
2.4 2.5	Электронная подпись; протокол аутентификации; протокол подбрасывания монеты по телефону; электронное голосование; электронные торги.	4
2.6	Схема Шамира; криптосистема Рабина; криптосистема Эль-Гамаля.	2
2.7 2.8	Эллиптические кривые; группы точек на эллиптических кривых; криптосистемы на эллиптических кривых.	4
2.9	Целочисленная арифметика многократной точности; расширенный двоичный НОД; сложение, вычитание, умножение, возведение в степень слева-направо и справа-налево.	2
2.10	Редукция Монтгомери, возведение в степень по Монтгомери.	2
	Лабораторные работы	8
ЛР2.1	Реализация схемы RSA.	4

ЛР2.2	Схема Шамира. Криптосистема Эль-Гамаля.	4
	Самостоятельная работа	27
СР2.1	Проработка учебного материала лекций	2.5
СР2.2	Подготовка к лабораторным работам	4
СР2.3	Подготовка к рубежному контролю	3
СР2.4	Другие виды самостоятельной работы	17.5
З	Экзамен	30
СР3.1	Подготовка к экзамену	30

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная работа студентов по дисциплине обеспечивается следующими учебно-методическими материалами:

1. Рабочая программа дисциплины.
2. Учебная литература и дополнительные материалы [Раздел 7 Рабочей программы дисциплины].
3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» [Раздел 8 Рабочей программы дисциплины].
4. Методические указания для обучающихся по освоению дисциплины [Раздел 9 Рабочей программы дисциплины], обеспечивающие самостоятельную работу студента при подготовке к учебным занятиям, выполнении домашних работ, подготовке к контрольным мероприятиям и аттестациям.
5. Комплект индивидуальных заданий.

Студенты получают доступ к указанным материалам начиная с первого занятия по дисциплине.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств (ФОС) для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине базируется на перечне компетенций с указанием этапов их формирования в процессе освоения образовательной программы (раздел 1). ФОС обеспечивает объективный контроль достижения всех результатов обучения, запланированных для дисциплины.

ФОС включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, владений и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания знаний, умений, владений и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Контроль освоения дисциплины производится в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации студентов МГТУ им. Н.Э. Баумана.

ФОС является приложением к данной рабочей программе дисциплины.

7. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И ДОПОЛНИТЕЛЬНЫХ МАТЕРИАЛОВ, НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Литература по дисциплине

1. Криптография и безопасность сетей Учебное пособие для СПО / Фороузан Б.А.
2. Алгебраическая криптография Монография / Романьков В.А.
3. Адаменко М. В. Основы классической криптологии: секреты шифров и кодов / Адаменко М. В. - М. : ДМК Пресс, 2012. - 253 с. : ил. - ISBN 978-5-94074-456-6.
4. Зубов А. Ю. Совершенные шифры. Дополнительные главы курса криптографии / Зубов А. Ю. - М. : Гелиос-АРВ, 2003. - 160 с. - Библиогр.: с. 157-159. - ISBN 5-85438-076-5.Теория чисел в криптографии : учеб. пособие для вузов / Орлов В. А., Медведев Н. В., Шимко Н. А., Домрачева А. Б. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2011. - 223 с. - Библиогр.: с. 221. - ISBN 978-5-7038-3520-3.
5. Практическая криптография М. Масленников / Масленников М.
6. Рябко Б. П., Фионов А. Н. Криптографические методы защиты информации : учеб. пособие для вузов / Рябко Б. П., Фионов А. Н. - 2-е изд., стер. - М. : Горячая линия - Теклеком, 2017. - 229 с. - (Учеб. пособие для вузов. Специальность). - Библиогр.: с. 218-221. - ISBN 978-5-9912-0286-2.

Дополнительные материалы

7. Практическая криптография: алгоритмы и их программирование / Аграновский А.В.; Хади Р.А.
8. Беломойцев Д. Е., Волосатова Т. М., Родионов С. В. Основные методы криптографической обработки данных : учеб. пособие / Беломойцев Д. Е., Волосатова Т. М., Родионов С. В. ; МГТУ им. Н. Э. Баумана. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2014. - 76 с. : ил. - Библиогр. в конце брош. - ISBN 978-5-7038-3833-4.
9. Основы криптографии Учебное пособие / Басалова Г.В.

8. ПЕРЕЧЕНЬ РЕСУРСОВ СЕТИ ИНТЕРНЕТ, РЕКОМЕНДУЕМЫХ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРИ ОСВОЕНИИ ДИСЦИПЛИНЫ

1. Сайт кафедры «Прикладная математика, информатика и вычислительная техника»: https://mf.bmstu.ru/info/faculty/kf/caf/k3/
2. Российская государственная библиотека. http://www.rsl.ru.
3. Государственная публичная научно-техническая библиотека России. http://www.gpntb.ru.
4. Библиотека МГТУ им. Н.Э. Баумана. http://library.bmstu.ru.
5. Научно-техническая библиотека КФ МГТУ им. Н.Э. Баумана. http://library.bmstu-kaluga.ru.
6. Научная электронная библиотека http://eLIBRARY.RU.
7. Электронно-библиотечная система издательства «Лань» http://e.lanbook.com.
8. Электронно-библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru.
9. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru.
10. Электронно-библиотечная система (ЭБС) «Юрайт» https://biblio-online.ru.
11. Центральная библиотека образовательных ресурсов Минобрнауки РФ. www.edulib.ru.
12. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru.
13. Федеральный центр информационно-образовательных ресурсов. http://fcior.edu.ru.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приступая к работе, каждый студент должен принимать во внимание нижеследующие положения.

Дисциплина построена по модульному принципу, каждый модуль представляет собой логически завершенный раздел курса. Дисциплина делится на три модуля (включая экзамен).

На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов по дисциплине.

Лекционные занятия посвящены рассмотрению ключевых, базовых положений курса и разъяснению учебных заданий, выносимых на самостоятельную проработку.

Лабораторные работы предназначены для приобретения опыта практической реализации основной профессиональной образовательной программы. Методические указания к лабораторным работам прорабатываются студентами во время самостоятельной подготовки. Необходимый уровень подготовки контролируется перед проведением лабораторных работ.

Практическая подготовка при реализации учебной дисциплины организуется путем проведения лабораторных работ и индивидуальных и(или) групповых консультаций, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка может включать в себя отдельные занятия лекционного типа, которые предусматривают передачу учебной информации обучающимся, необходимой для последующего выполнения работ, связанных с будущей профессиональной деятельностью.

Самостоятельная работа студентов включает следующие виды: проработка учебного материала лекций, подготовка к лабораторным работам, подготовка к экзамену, подготовка к рубежному контролю. Результаты всех видов работы студентов формируются в виде их личного рейтинга, который учитывается на промежуточной аттестации. Самостоятельная работа предусматривает не только проработку материалов лекционного курса, но и их расширение в результате поиска, анализа, структурирования и представления в компактном виде современной информации из всех возможных источников.

Текущий контроль проводится в течение каждого модуля, его итоговые результаты складываются из оценок по следующим видам контрольных мероприятий:

- Рубежный контроль;
- Лабораторные работы.

Освоение дисциплины и ее успешное завершение на стадии промежуточной аттестации возможно только при регулярной работе во время семестра и планомерном прохождении текущего контроля. Набрать рейтинг по всем модулям в каждом семестре, пройти по каждому модулю плановые контрольные мероприятия в течение экзаменационной сессии невозможно.

Для завершения работы в семестре студент должен выполнить все контрольные мероприятия.

Промежуточная аттестация по дисциплине проходит в форме экзамена, контролирующего освоение ключевых, базовых положений дисциплины, составляющих основу остаточных знаний по ней.

Методика оценки по рейтингу

Студент, выполнивший все предусмотренные учебным планом задания и сдавший все контрольные мероприятия, получает итоговую оценку по дисциплине за семестр в соответствии со шкалой:

Рейтинг	Оценка на экзамене
85 – 100	отлично
71 – 84	хорошо

60 – 70	удовлетворительно
0 – 59	неудовлетворительно

Оценивание дисциплины ведется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации студентов МГТУ им. Н.Э. Баумана.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ И ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ

Информационные технологии:

– Электронная информационно-образовательная среда МГТУ им. Н.Э. Баумана обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик, формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы. Предусмотрена возможность синхронного и асинхронного взаимодействия студентов и преподавателей посредством технологий и служб по пересылке и получению электронных сообщений между пользователями компьютерной сети Интернет.

– e-mail преподавателя для оперативной связи: vetoshkin@bmstu.ru

Программное обеспечение:

– Mathcad

Информационные справочные системы:

– Информационно-правовая система «Гарант» http://www.garant.ru;
– Информационно-правовая система «Консультант Плюс» http://www.consultant.ru/

Профессиональные базы данных:

– Ресурс «Машиностроение» http://www.i-mash.ru.
– Портал машиностроения http://www.mashportal.ru.

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Перечень материально-технического обеспечения дисциплины

№, п/п	Вид занятий	Вид и наименование оборудования
1	Лекции	специально оборудованные аудитории с мультимедийными средствами, средствами звуковоспроизведения и имеющими выход в сеть Интернет; помещения для проведения аудиторных занятий, оборудованные учебной мебелью; аудитории оснащенные компьютерами с доступом к базам данных и сети Интернет; студии; компьютерные классы.
2	Лабораторные работы	специально оборудованные аудитории с мультимедийными средствами, средствами звуковоспроизведения и имеющими выход в сеть Интернет; помещения для проведения аудиторных занятий, оборудованные учебной мебелью; аудитории оснащенные компьютерами с доступом к базам данных и сети Интернет; студии; компьютерные классы.
3	Самостоятельная работа	библиотека, имеющая рабочие места для студентов; выставочные залы; аудитории, оснащенные компьютерами с доступом к сети Интернет. Социокультурное пространство университета позволяет студенту качественно выполнять самостоятельную работу.

Утверждена на заседании кафедры К3

«Прикладная математика, информатика и вычислительная техника»

Протокол № 9 от 15.04.2022 г.

ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ

1). П.7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ЧИТАТЬ В СЛЕДУЮЩЕЙ РЕДАКЦИИ:

7. Перечень учебной литературы и дополнительных материалов, необходимых для освоения дисциплины

Литература по дисциплине:

1. Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 с. — ISBN 978-5-97060-166-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/82817
2. Практическая криптография М. Масленников / Масленников М. - URL: https://ibooks.ru/reading.php?short=1&productid=335092.
3. Теория чисел в криптографии : учеб. пособие для вузов / Орлов В. А., Медведев Н. В., Шимко Н. А., Домрачева А. Б. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2011. - 223 с. - Библиогр.: с. 221. - ISBN 978-5-7038-3520-3.
4. Криптографические методы защиты информации / Аверченков В.И., Рытов М.Ю., Шпичак С.А. - 2017. - URL: https://znanium.com/catalog/document?id=358088.
5. Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - 2016. - URL: http://www.iprbookshop.ru/90248.html.
6. Беломойцев, Д. Е. Основные методы криптографической обработки данных : учебное пособие / Д. Е. Беломойцев, Т. М. Волосатова, С. В. Родионов. — Москва : МГТУ им. Н.Э. Баумана, 2014. — 76 с. — ISBN 978-5-7038-3833-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/58438
7. Основы криптографии Учебное пособие / Басалова Г.В. - 2020. - URL: http://www.iprbookshop.ru/89455.html.
8. Криптография и безопасность сетей Учебное пособие для СПО / Фороузан Б.А. - 2021. - URL: http://www.iprbookshop.ru/102192.html.
9. Алгебраическая криптография Монография / Романьков В.А. - 2013. - URL: http://www.iprbookshop.ru/24868.html.

2). П.10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ЧИТАТЬ В СЛЕДУЮЩЕЙ РЕДАКЦИИ:

10. Перечень информационных технологий, используемых при изучении дисциплины, включая перечень программного обеспечения, информационных справочных систем и профессиональных баз данных

Программное обеспечение:
- Mathcad

Преподаватель кафедры:

Ветошкин А.М., доцент (к.н.), кандидат технических наук, доцент, lapashina@bmstu.ru

Утверждена на заседании кафедры К3

«Прикладная математика, информатика и вычислительная техника»

Протокол № 9 от 14.04.2023 г.

ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ

1). П.7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ЧИТАТЬ В СЛЕДУЮЩЕЙ РЕДАКЦИИ:

7. Перечень учебной литературы и дополнительных материалов, необходимых для освоения дисциплины

Литература по дисциплине:

1. Теория чисел в криптографии : учеб. пособие для вузов / Орлов В. А., Медведев Н. В., Шимко Н. А., Домрачева А. Б. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2011. - 223 с. - Библиогр.: с. 221. - ISBN 978-5-7038-3520-3.
2. Беломойцев, Д. Е. Основные методы криптографической обработки данных : учебное пособие / Д. Е. Беломойцев, Т. М. Волосатова, С. В. Родионов. — Москва : МГТУ им. Н.Э. Баумана, 2014. — 76 с. — ISBN 978-5-7038-3833-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/58438
3. Основы криптографии Учебное пособие / Басалова Г.В. - 2020. - URL: http://www.iprbookshop.ru/89455.html.
4. Криптография и безопасность сетей Учебное пособие для СПО / Фороузан Б.А. - 2021. - URL: http://www.iprbookshop.ru/102192.html.
5. Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 с. — ISBN 978-5-97060-166-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/82817
6. Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - 2016. - URL: http://www.iprbookshop.ru/90248.html.

2). П.10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ЧИТАТЬ В СЛЕДУЮЩЕЙ РЕДАКЦИИ:

10. Перечень информационных технологий, используемых при изучении дисциплины, включая перечень программного обеспечения, информационных справочных систем и профессиональных баз данных

Программное обеспечение:

- Mathcad

Преподаватель кафедры:

Ветошкин А.М., доцент (к.н.), кандидат технических наук, доцент, vetoshkin@bmstu.ru

Утверждена на заседании кафедры К3

«Прикладная математика, информатика и вычислительная техника»

Протокол № 9 от 18.04.2024 г.

ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ

1). П.7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ЧИТАТЬ В СЛЕДУЮЩЕЙ РЕДАКЦИИ:

7. Перечень учебной литературы и дополнительных материалов, необходимых для освоения дисциплины

Литература по дисциплине:

1. Теория чисел в криптографии : учеб. пособие для вузов / Орлов В. А., Медведев Н. В., Шимко Н. А., Домрачева А. Б. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2011. - 223 с. - Библиогр.: с. 221. - ISBN 978-5-7038-3520-3.
2. Беломойцев, Д. Е. Основные методы криптографической обработки данных : учебное пособие / Д. Е. Беломойцев, Т. М. Волосатова, С. В. Родионов. — Москва : МГТУ им. Н.Э. Баумана, 2014. — 76 с. — ISBN 978-5-7038-3833-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/58438
3. Криптография и безопасность сетей Учебное пособие для СПО / Фороузан Б.А. - 2021. - URL: http://www.iprbookshop.ru/102192.html.
4. Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 с. — ISBN 978-5-97060-166-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/82817
5. Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - 2016. - URL: http://www.iprbookshop.ru/90248.html.

2). П.10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ЧИТАТЬ В СЛЕДУЮЩЕЙ РЕДАКЦИИ:

10. Перечень информационных технологий, используемых при изучении дисциплины, включая перечень программного обеспечения, информационных справочных систем и профессиональных баз данных

Программное обеспечение:

- Mathcad

Преподаватель кафедры:

Ветошкин А.М., доцент (к.н.), кандидат технических наук, доцент, vetoshkin@bmstu.ru