МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра математики и физики

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ Е.И. Луковникова
«_____» декабря 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Б1.В.16

НАПРАВЛЕНИЕ ПОДГОТОВКИ

01.03.02 Прикладная математика и информатика

ПРОФИЛЬ ПОДГОТОВКИ

Инженерия программного обеспечения

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

СОДЕРЖАНИЕ ПРОГРАММЫ **Стр.**

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Вид деятельности выпускника

Дисциплина охватывает круг вопросов, относящихся к научно – исследовательскому, проектному и производственно-технологическому виду профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Целью изучения дисциплины является: ознакомление обучающихся с математическими основами современной криптографии, принципами защиты информации с помощью криптографических методов и способов реализации этих методов на практике.

Задачи дисциплины

Освоение студентом:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- принципов синтеза и анализа шифров;
- математических методов, используемых в криптоанализе.

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ПК-2	способность понимать, совершенствовать и применять современный математический аппарат	**знать:** - приемы самостоятельного изучения криптографических методов; - анализ сильных и слабых мест в используемых алгоритмах. **уметь:** - выбрать подходящий алгоритм для заданной задачи. **владеть:** – навыками решения задач из разных областей криптографии;
ПК-3	способность критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности	**знать:** - сильные и слабые стороны используемого алгоритма. **уметь:** - самостоятельно выбирать методы и приемы при решении криптографических, математических и логических задач; **владеть:** – приемами анализа результатов решения и сопоставления с конкретной ситуацией.
ПК-4	способность работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности	**знать:** источники формирования информационной базы, характеризующей функционирование экономических систем в сфере международной торговли и внешнеэкономических связей; **уметь:** использовать источники экономической, социальной, управленческой информации для анализа экономических процессов, выявления проблем и определения способов их решения; **владеть:** навыками сбора, анализа и обработки данных для решения текущих и стратегических

		внешнеэкономических задач.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.16 Криптографические методы защиты информации относится к вариативной части.

Дисциплина Криптографические методы защиты информации базируется на знаниях, полученных при изучении дисциплин: Основы информатики, Теория алгоритмов, Линейное и нелинейное программирование, Комплексный анализ, Языки и методы программирования, Математическое моделирование, Базы данных и Теория информации и кодирования. Криптография представляет основу для изучения дисциплин: Технические средства и методы защиты информации.

Такое системное междисциплинарное изучение направлено на достижение требуемого ФГОС уровня подготовки по квалификации бакалавр.

3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ

3.1. Распределение объема дисциплины по формам обучения

Форма обучения	***Курс***	***Семестр***	***Трудоемкость дисциплины в часах***						***Контрольная работа***	***Вид промежуточной аттестации***
			Всего часов (с экз.)	***Аудиторных часов***	***Лекции***	***Лабораторные работы***	***Практические занятия***	***Самостоятельная работа***		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Очная	4	7	144	68	17	51	-	31	кр	Экзамен
Заочная	-	-	-	-	-	-	-	-	-	-
Заочная (ускоренное обучение)	-	-	-	-	-	-	-	-	-	-
Очно-заочная	-	-	-	-	-	-	-	-	-	-

3.2. Распределение объема дисциплины по видам учебной работы, включая самостоятельную работу обучающихся и трудоемкость

Вид учебных занятий	*Трудоемкость (час.)*	*в т.ч. в интерактивной, активной, инновационной формах, (час.)*	*Распределение по семестрам, час*
			7
1	2	3	4
I. Контактная работа обучающихся с преподавателем (всего)	68	-	68
Лекции (Лк)	17	-	17
Лабораторные работы (ЛР)	51	-	51
Контрольная работа	+	-	+
Групповые (индивидуальные) консультации	+	-	+
II.Самостоятельная работа обучающихся (СР)	31	-	31
Подготовка к лабораторным работам	10	-	10
Подготовка к экзамену в течение семестра	10	-	10
Выполнение контрольной работы	11	-	11
III. Промежуточная аттестация экзамен	45	-	45
Общая трудоемкость дисциплины ……. час.	144	-	144
зач. ед.	4	-	4

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий
- для очной формы обучения:

№ раздела и темы	*Наименование раздела и тема дисциплины*	*Трудоемкость, (час.)*	*Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)*		
			учебные занятия		*самостоятельная работа обучающихся**
			лекции	*лабораторные работы*	
1	2	3	4	5	6
1.	**Введение в криптографию. Математические операции в криптографии**	**20**	**6**	**-**	**14**
1.1.	Введение в криптографию	4	2	-	2
1.2	Шифры	8	2	-	6
1.3	Математические операции в криптографии	8	2	-	6
2.	**Системы шифрования**	**47**	**6**	**31**	**10**
2.1.	Системы симметричного шифрования	24	3	16	5
2.2	Системы асимметричного	23	3	15	5

	шифрования				
3.	**Хеш-функции**	**32**	**5**	**20**	**7**
3.1	Понятие Хеш-функции	15	2	10	3
3.2	Цифровая подпись	17	3	10	4
	ИТОГО	**99**	**17**	**51**	**31**

4.2. Содержание дисциплины, структурированное по разделам и темам

№ раздела и темы	*Наименование раздела и темы дисциплины*	*Содержание лекционных занятий*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**2**	**3**	**4**
1.	**Введение в криптографию**		-
1.1.	Введение в криптографию	Принципы построения криптографических алгоритмов. История криптографии: Основные этапы становления криптографии как науки. Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их модели и свойства. Основные понятия криптографии: Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	-
1.2.	Шифры	Ручные и машинные шифры. Основные требования к шифрам. Шифры перестановки. Шифры замены. Поточные шифры. Надежность шифров. Имитостойкость шифров. Помехоустойчивость шифров.	-
1.3	Математические операции в криптографии	Раздел математики развившие криптографию. Теория кодирования. Булева алгебра. Теория алгоритмов. Математический анализ. Классические шифры. Стойкость теоретическая и практическая	-
2.	**Системы шифрования**		-
2.1	Системы симметричного шифрования	Общая модель. Классические системы: простая перестановка, одиночная перестановка по ключу, двойная перестановка, перестановка "Магический квадрат".	-
2.2	Системы асимметричного шифрования	Системы шифрования: ГОСТ 28147-89, DES, AES.	-
3.	**Хеш-функции**		-
3.1	Понятие Хеш-функции	Понятие Хеш-функции. Общая модель. Системы шифрования на основе односторонних функций RSA. Обмен ключами Диффи-Хелмана. Шифрование Эль Гамаля.	-
3.2	Цифровая подпись	Цифровая подпись. Функция проверки подписи. Модели атак и их возможные результаты. Управление открытыми ключами. Хранение закрытого ключа.	-

4.3 Лабораторные работы

№ п/п	*Номер раздела дисциплины*	*Наименование лабораторных работ*	*Объем в часах*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**2.**	Шифр: Атбаш, Цезаря, Замена на цифры, Квадрат Полибия, Азбука морзе, шифр Энигма.	10	-
2		Работа с ГОСТ 28147-89 и режимами: ECB, CBC, CFB, OFB.	11	-
3		Решение задач шифрами: RSA, Эль Гамаля и Рабина.	10	-
4	**3.**	Работа с хеш протаколами.	10	-
5		Работа с квантовой криптографией	10	-
		ИТОГО	**51**	

4.4 Практические занятия

Учебным планом не предусмотрено.

4.5 Контрольные мероприятия: контрольная работа

Контрольная работа « Синтез и анализ криптографических шрифтов».

Цель: Сформировать у учащихся умения

- по заданному варианту (симметричных и ассиметричных шифров) воссоздать шифр, разобравшись в его основах и операциях, для шифрации и дешифрации сообщений;

- уметь охарактеризовать его мощность ключевого пространства, сложность по пространству и времени, защищенность от традиционного и квантового криптоанализа, защищенность от различных атак.

№	**Виды шифров:**
1	ГОСТ – 28147-89
2	DES
3	Шифр на элептических кривых
4	Mc Eliece
5	IDEA
6	AES
7	Twofish
8	Camellia
9	РСЛОС
10	Rijndael

Содержание. Виды заданий: №1 – по данной таблице выбрать шифр, №2 – изучить данный вид шифрования (его структуру, состав, примеры), №3 – воспроизвести данный шифр в программном виде (на любом языке программирования), №4 – осуществить проверку на каждом этапе его работы, №5 – осуществить шифрацию сообщения через программу, №6 - провести дешифрацию и доказать правильность шифра, №7 - изучить способы и методы его взлома, №8 – сделать вывод о криптостойкости данного шифра.

Структура: Контрольная работа выполняется в трех частях. В первом разделе описывается теория о шифре. Во второй части представить работу элементов шифра с указанием программного кода данного этапа и его проверка. В третьей части представить описание про-

граммы (с иллюстрациями) и привести шифрацию текста и дешифрацию шифртекста через программу.

Рекомендуемый объём: не более 30 страниц.

Выдача задания, прием кр и защита проводится в соответствии с календарным учебным графиком.

Оценка	**Критерии оценки контрольной работы**
отлично	Выполнены все необходимые задания и написана программа.
хорошо	Выполнены все необходимые задания, но программа реализована не до конца.
удовлетворительно	Выполнены все необходимые задания, но программа реализована не вся (не все этапы шифра).
неудовлетворительно	Не изучен алгоритм, или не написана программа.

5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ ПРОФЕССИОНАЛЬНЫМ, ОБЩЕКУЛЬТУРНЫМ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Компетенции / ***№, наименование разделов дисциплины***	***Кол-во часов***	***Компетенции***			***Σ комп.***	***tср, час***	***Вид учебной работы***	***Оценка результатов***
		ПК						
		2	***3***	***4***				
1	**2**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1. Введение в криптографию	22	+	+	+	3	7,33	Лк, ЛР	кр, экзамен
2. Системы шифрования	40	+	+	+	3	13,33	Лк, ЛР	кр, экзамен
3. Хеш-функции	37	+	+	+	3	12,33	Лк, ЛР	кр, экзамен
всего часов	**99**	**33**	**33**	**33**	**3**	**33**		

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1.Смарт, Н. Криптография: учебное пособие/Н. Смарт; пер. с англ. – М.:Техносфера, 2006. – 528 с.

2. Молдовян, Н.А., Введение в криптосистемы с открытым ключом: учебное пособие/ Н.А. Молдовян. – С-Пб.: «БХВ-Петербург», 2005. - 286 с.

3. Левин, М. Криптография без секретов: руководство пользователя/М. Левин. — М.: Новый издательский дом, 2005. — 320 с.

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№	*Наименование издания*	***Вид занятия*** *(Лк, ЛР, кр)*	***Количество экземпляров в библиотеке,*** **шт.**	***Обеспеченность,*** **(экз./ чел.)**
1	2	3	4	5
Основная литература				
1.	Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информ-вционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689	Лк, ЛР, кр	1 (ЭУ)	1
2.	Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092	Лк, ЛР, кр	1 (ЭУ)	1
Дополнительная литература				
3.	Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605	Лк, ЛР, кр	1 (ЭУ)	1

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В процессе обучения студенты могут использовать общие ресурсы:

1.Электронный каталог библиотеки БрГУ http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=.

2. Электронная библиотека БрГУ http://ecat.brstu.ru/catalog .

3. Электронно-библиотечная система «Университетская библиотека online» http://biblioclub.ru .

4. Электронно-библиотечная система «Издательство «Лань» http://e.lanbook.com .

5. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru .

6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru .

7. Университетская информационная система РОССИЯ (УИС РОССИЯ) https://uisrussia.msu.ru/ .
8. Национальная электронная библиотека НЭБ
http://xn--90ax2c.xn--p1ai/how-to-search /.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Обучающийся должен разработать собственный режим равномерного освоения дисциплины. Подготовка студента к предстоящей лекции включает в себя ряд важных познавательно-практических этапов:

– чтение записей, сделанных в процессе слушания и конспектирования предыдущей лекции, вынесение на поля всего, что требуется при дальнейшей работе с конспектом и учебником;

– техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств);

– выполнение практических заданий преподавателя;

– знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе.

Практическое занятие по математике позволяет студенту более глубоко разобраться в теоретическом материале и определить сферы его практического применения. Основная цель практического занятия – развитие самостоятельности студента.

Контрольные мероприятия представляют собой способ проверки знаний студента, его умений и предполагают письменные ответы на поставленные вопросы, либо самостоятельное выполнение практических заданий. Подготовка к контрольным мероприятиям состоит в ответственном выполнении всех домашних заданий по дисциплине и самостоятельной проработке основной и дополнительной литературы.

Наиболее продуктивной является самостоятельная работа в библиотеке, где доступны основные и дополнительные печатные и электронные источники.

При выполнении приведенных выше рекомендаций подготовка к зачету и экзамену сведется к повторению изученного и совершенствованию навыков применения теоретических положений и различных методов решения к стандартным и нестандартным заданиям.

9.1. Методические указания для обучающихся по выполнению лабораторных работ

Лабораторная работа №1

Шифр: Атбаш, Цезаря, Замена на цифры, Квадрат Полибия, Азбука морзе, Энигма.

Цель работы:

Изучить простые шифры криптографии, написать ряд программ и решить логическую задачу.

Задание:

1) По шифру Цезаря расшифровать фразу: Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб.

2) Зашифруйте вручную свои ФИО по шифрам: Цезаря, Атбаш, замена букв на числа по их местоположению в русском алфавите (например: а(1), б(2)…).

3) Разбиться на команды по 2 человека и написать программы реализующие шифрование и расшифрование шифров (кто работает в одиночку выбрать любые три шифра):

- Атбаш;
- Цезарь;
- Замена на цифры;
- Квадрат Полибия;
- Азбука морзе;
- Энигма.

4) Решить задачу. На одной улице стоят в ряд 4 дома, в которых живут 4 человека: Алексей, Егор, Виктор и Михаил. Известно, что каждый из них владеет ровно одной из следующих профессий: Токарь, Столяр, Хирург и Окулист, но неизвестно, кто какой, и неизвестно, кто в каком доме живет. Однако известно, что:

- Столяр живет правее Хирурга
- Окулист живет левее Хирурга
- Токарь живет с краю
- Токарь живет рядом с Окулистом
- Егор не Токарь и не живет рядом с Токарем
- Михаил живет рядом с Хирургом
- Алексей живет правее Окулиста
- Алексей живет через дом от Михаила

Выясните, кто какой профессии, и кто где живет. Ответ доказать.

Порядок выполнения:

1. Изучить теоретические сведения и примеры.
2. Решить предложенные задачи и написать ряд программ.
3. Произвести проверку полученных результатов.

Форма отчетности:

Составить отчет на листах формата А4 с описанием решения задач и скриншотов написанных программ (последние можно реализовать на любом построителе).

Рекомендации по выполнению заданий и подготовке к практическому занятию

Подготовка к практическим занятиям состоит в добросовестном анализе теоретического материала, составлении кратких справочников, словариков, схем, алгоритмов. Если во время подготовки к лабораторной работе возникли трудности в освоении учебного материала, то необходимо подготовить вопросы преподавателю, раскрывающие их.

Для выполнения лабораторного задания необходимо найти нужные шифры и изучить их структуру, повторить основы работы с программными построителями и составить алгоритмы решения задач.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1) Определение и основные понятия криптографии.
2) Периоды развития шифровального дела.
3) Основные требования к шифрам.
4) Надежность шифра.
5) Имитостойкость и помехоустойчивость шифров.
6) Криптография в России.
7) Использование математики в криптографии.

Лабораторная работа №2

Работа с ГОСТ 28147-89 и режимами: ECB, CBC, CFB, OFB.

Цель работы:

Изучить работу симметричных алгоритмов.

Задание:

1) Напишите 2 программы по шифру «Одиночная перестановка по ключу» и по шифру «Магический квадрат» используя таблицу 5 на 5. Сообщение и ключевое слово каждый студент выбирает сам.

2) Зашифруйте свои ФИО по шифрам Виженера и Вернама, где ключевое слово каждый студент выбирает сам.

3) Выполните первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены в программном виде. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

4) Зашифруйте свои ФИО используя генератор ключей блочным шифром. Программу можно не писать, а найти в интернете.

- Electronic Codebook (ECB);
- Cipher Block Chaining (CBC);
- Cipher Feedback (CFB);
- Output Feedback (OFB).

Сравнить результаты всех 4-х режимов (при одинаковом ключе) и выбрать более надежный из них. Ответ аргументировать.

Порядок выполнения:

1. Изучить теоретические сведения и примеры с данными шифрами.
2. Решить предложенные задачи и написать программу по ГОСТ 28147-89.
3. Произвести проверку полученных результатов.

Форма отчетности:

Составить отчет на листах формата А4 с описанием решения задач и скриншотов написанных программ (последние можно реализовать на любом построителе).

Рекомендации по выполнению заданий и подготовке к практическому занятию

Подготовка к практическим занятиям состоит в добросовестном анализе теоретического материала, составлении кратких справочников, словариков, схем, алгоритмов. Если во время подготовки к лабораторной работе возникли трудности в освоении учебного материала, то необходимо подготовить вопросы преподавателю, раскрывающие их.

Для выполнения лабораторного задания необходимо найти нужные шифры и изучить их структуру, повторить основы работы с программными построителями и составить алгоритмы решения задач.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1)Дать определение и изобразить симметричную криптосистему.

2)Перечислить достоинства и недостатки таких систем.

3)Привести основные отличия поточных шифров от блочных.

4)В чем разница между синхронными и самосинхронизирующимися поточными шифрами.

5)Перечислить атаки на поточные шифры.

6)Рассказать о четырех режимах шифрования.

7)Как работает шифр Вернама и Виженера.

8)Отобразить схему ГОСТ 28147-89 и пояснить ее элементы.

9)Достоинства и трудности при работе с гостом.

10)Время жизни ключа и распределение ключа.

11)Принцип действия протокола Широкоротой лягушки.

12)Принцип действия протокола Отвэй-Риса.

13)Принцип действия протокола Цербер.

Лабораторная работа №3

Решение задач шифрами: RSA, Эль Гамаля и Рабина.

Цель работы:

Изучить работу асимметричных алгоритмов.

Задание:

1) Нужно зашифровать текст b = 780 используя алгоритм RSA. Студент сам выбирает значения p, g и d, не забывая про условия взаимной простоты. Результат проверить расшифровкой.

2) Нужно зашифровать текст (собственные ФИО студента) используя алгоритм RSA. Студент сам выбирает значения p, g и d, не забывая про условия взаимной простоты. Результат проверить расшифровкой.

3) Нужно зашифровать текст (собственные ФИО студента) используя алгоритм Эль Гамаля. Студент сам выбирает значения p, g и x_1, x_2. Результат проверить расшифровкой.

4) Нужно зашифровать текст M = 780 используя алгоритм Рабина. Студент сам выбирает значения p, g. Результат проверить расшифровкой.

Все задания выполнить в печатном виде, с представлением всех используемых формул.

Порядок выполнения:

1. Изучить теоретические сведения и примеры с данными шифрами.
2. Произвести проверку полученных результатов.

Форма отчетности:

Составить отчет на листах формата А4 с описанием решения задач.

Рекомендации по выполнению заданий и подготовке к практическому занятию

Подготовка к практическим занятиям состоит в добросовестном анализе теоретического материала, составлении кратких справочников, словариков, схем, алгоритмов. Если во время подготовки к лабораторной работе возникли трудности в освоении учебного материала, то необходимо подготовить вопросы преподавателю, раскрывающие их.

Для выполнения лабораторного задания необходимо найти нужные шифры и изучить их структуру, повторить основы работы с программными построителями и составить алгоритмы решения задач.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1) Дать определение асимметричным криптосистемам, назвать основные свойства и изобразить.

3) Какие достоинства и недостатки имеет данная система?

4) Изобразить и объяснить основные стратегии взлома систем.

5) Этапы выполнения и способы взлома шифра RSA.

7) Рассказать способ обмена клчами Деффи-Хелмана.

8) Этапы выполнения шифра Эль Гамаля.

9) Этапы выполнения шифра Рабина.

10) Рассказать об оценке шифров RSA, Эль Гамаля и Рабина.

Лабораторная работа №4

Работа с хеш протаколами.

Цель работы:

Изучить работу с хеш протаколами.

Задание:

1) Найти хеш–образ собственной Фамилии, используя хеш–функцию $H_i = (H_{i-1} + M_i)^2 \bmod n$, где n = pq, p и q – большие простые числа (таблица 3.1).

2) Используя хеш-образ собственной Фамилии, расчитайте электронную цифровую подпись используя схему RSA.

3) Каждому студенту выбрать по одному хэш протоколу (MD4, MD5, MDC, RIPEMD, SHS – можно взять и другие протоколы). Подробно его изучить (кто автор, режим работы, где используется, пример работы и др.). Написать программу, реализующую данный протокол.

Порядок выполнения:

1. Изучить теоретические сведения и примеры с данными шифрами.
2. Произвести проверку полученных результатов.

Форма отчетности:

Составить отчет на листах формата А4 с описанием решения задач.

Рекомендации по выполнению заданий и подготовке к практическому занятию

Подготовка к практическим занятиям состоит в добросовестном анализе теоретического материала, составлении кратких справочников, словариков, схем, алгоритмов. Если во время подготовки к лабораторной работе возникли трудности в освоении учебного материала, то необходимо подготовить вопросы преподавателю, раскрывающие их.

Для выполнения лабораторного задания необходимо найти нужные шифры и изучить их структуру, повторить основы работы с программными построителями и составить алгоритмы решения задач.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689

2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки

1) Дать определение электронной цифровой подписи, назвать достоинства и недостатки.

2) Что такое функция проверки подписи.
3) Цифровая подпись RSA и его недостатки.
4) Рассказать о цифровой подписи DSA.
5) Модели атак и их результаты на цифровые подписи.
6) Как осуществляется управление открытыми ключами.
7) Как происходит хранение закрытого ключа.
8) Дать определение Хэш-функции (или хешированию).
9) Назвать условия использования хэш-функций.
10) Перечислить ключевые характеристики ХЭШ алгоритмов.
11) Рассказать о протоколе MD4 и MD5.
12) Рассказать о протоколе MDC и RIPEMD.

Лабораторная работа №5

Работа с квантовой криптографией.

Цель работы:

Изучить способы с квантовой криптографией.

Задание:1) Зашифровать и расшифровать ФИО алгоритмом GGH. Матрицы B и U взять из примера (можно рассчитать самим). Представить свою ФИО в виде матрицы сообщения m, следующим образом: заменить все буквы на их номера в алфавите, первая строка матрицы – фамилия, вторая – имя и третья – отчество, к недостающим значениям (в столбцах) добавить нули, для выравнивания. Например:

$$m = \begin{pmatrix} 21 & 3 & 5 & 12 & 9 \\ 32 & 1 & 27 & 0 & 0 \\ 22 & 20 & 10 & 6 & 0 \end{pmatrix}.$$

2) Каждому студенту выбрать по одному алгоритму квантовой криптографии. Подробно изучить (кто автор, режим работы, где используется, пример работы и др.). Написать программу, реализующую данный алгоритм.

Порядок выполнения:

1. Изучить теоретические сведения и примеры с данными шифрами.
2. Произвести проверку полученных результатов.

Форма отчетности:

Составить отчет на листах формата А4 с описанием решения задач.

Рекомендации по выполнению заданий и подготовке к практическому занятию

Подготовка к практическим занятиям состоит в добросовестном анализе теоретического материала, составлении кратких справочников, словариков, схем, алгоритмов. Если во время подготовки к лабораторной работе возникли трудности в освоении учебного материала, то необходимо подготовить вопросы преподавателю, раскрывающие их.

Для выполнения лабораторного задания необходимо найти нужные шифры и изучить их структуру, повторить основы работы с программными построителями и составить алгоритмы решения задач.

Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций/ Г.В. Басалова; Национальный открытый университет «ИНТУИТ». – М.: Интернет – Университет Информвционных Технологий, 2011. – 253 с.; [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=233689
2. Лапонина О.Р. Криптиграфические основы безопасности/О.Р. Лапонина.- М.: Национальный открытый университет «ИНТУИТ»., 2016. – 244 с. [Электронный ресурс]. http://biblioclub.ru/index.php?page=book&id=429092

Дополнительная литература

3 Артемов А.А. Информационная безопасность: курс лекций [Электронный ресурс]/ А.А. Артемов.-Орел: МАБИВ, 2014 – Электр. опт. диск (CD-ROM) http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

Контрольные вопросы для самопроверки:

1) Аутентификация (определение и методы).
2) Аутентификации по уровню информационной безопасности.
3) Информационная безопасность РФ.
4) Угроза информационной безопасности.
5) Направления защиты информации.
6) Система защиты информации.
7) Структура информационного противоборства.
8) Электронные платежи.
9) Проблемы современной криптографии.
10) Новые технологии в криптоанализе.

9.2. Методические указания по выполнению контрольной работы

Контрольная работа представляет собой способ проверки знаний студента, его умений и предполагают письменные ответы на поставленные вопросы, либо самостоятельное выполнение практических заданий. Подготовка к контрольной работе состоит в ответственном выполнении всех домашних заданий по дисциплине и самостоятельной проработке основной и дополнительной литературы.

Целью контрольной работы является приобретение навыков самостоятельной работы с литературой, закрепление умений работы со средой программирования, формирование навыков оценки результатов собственной деятельности.

Выполнения контрольной работы предполагает:

- анализ поставленных задач и выбор методов их решения;
- реализацию решения поставленных задач;
- проверку и анализ полученных результатов;
- оформление отчета.

Отчет по контрольной работе оформляется в печатном виде и содержит:

- формулировку заданий;
- описание их решений;
- полученные результаты;
-выводы.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

ОС Windows 7 Professional
Microsoft Office 2007 Russian Academic OPEN No Level
Антивирусное программное обеспечение Kaspersky Security.

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Вид занятия (*Лк, Лр , кр)*	***Наименование аудитории***	***Перечень основного оборудования***	***№ Лр***
1	**3**	**4**	**5**
Лк	Лекционная аудитория		№ 1.1 -3.2
ЛР	Лаборатория технических средств защиты информации	Оборудование 16-ПК i5-2500/H67/4Gb/500Gb (монитор TFT19 Samsung E1920NR); интерактивная доска Smart Board X885ix со встроенным проектором UX60	№ 1-5
кр	Читальный зал №1	Оборудование 10 ПК i5-2500/H67/4Gb(монитор TFT19 Samsung); принтер HP LaserJet P2055D	-
СР	Читальный зал №1		-

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-2	Способность понимать, совершенствовать и применять математический аппарат	1. Введение в криптографию. Математические операции в криптографии	1.1 Введение в криптографию	Вопросы к экзамену 1-2
			1.2 Шифры	Вопросы к экзамену 3-4
			1.3 Математические операции в криптографии	Вопросы к экзамену 5
		2. Системы шифрования	2.1 Системы симметричного шифрования	Вопросы к экзамену 6-13
			2.2 Системы асимметричного шифрования	Вопросы к экзамену14-17
ПК-3	Способность критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности	3. Хеш-функции	3.1 Понятие Хеш-функции	Вопросы к экзамену 18
			3.2 Цифровая подпись.	Вопросы к экзамену 19-22
ПК-4	способностью работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности			

2. Вопросы к экзамену

№ п/п	Компетенции		ЭКЗАМЕННАЦИОННЫЕ ВОПРОСЫ 3 семестр	№ и наименование раздела
	Код	Определение		
1	2	3	4	5
1. 2.	ПК-2	Способность понимать, совершенствовать и применять математический аппарат	1. Определение и основные понятия криптографии. Алгоритм шифрования.	1. Введение в криптографию. Математические операции в криптографии
			2. Периоды развития шифровального дела. Древние шифры (не меньше 5).	
			3. Криптография в России. Основные требования к шифрам.	
			4. Надежность шифра. Имитостойкость и помехоустойчивость шифров.	
			5. Алгоритмы. Свойства алгоритмов. Требования к алгоритмам.	
			6. Симметричные криптосистемы (определение, схема, достоинства и недостатки).	2. Системы шифрования
			7. Простая перестановка. Одиночная перестановка по ключу. Магический квадрат.	
			8. Блочные шифры. Поточные шифры. Атаки на шифры (3 вида)	
			9. Режимы работы блочного шифра: ECB и CBC (описание, формула и чертеж).	
			10. Режимы работы блочного шифра: CFB и OFB (описание, формула и чертеж).	
			11. Шифр Виженера. Шифр Вернама. Шифр DES.	
			12. ГОСТ 28147-89 (4 режима, схемы, достоинства и недостатки).	
			13. Шифр AES. Протоколы: Широкоротой лягушки, Отвэй-Риса и Цербер.	
			14. Асимметричные криптосистемы (определение, схема, свойства, достоинства и недостатки).	
3.	ПК-3	Способность критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности	15. Возможности взлома ас. шифров. Квантовая криптография.	
			16. Шифр RSA (схема, способы взлома). Обмен ключами Диффи-Хелмана.	
			17. Шифр Эль Гамаля. Шифр Рабина.	
			18. Хэш-функции (определение, назначение, условия использования).	3. Хеш-функции
			19. Электронная цифровая подпись. Подпись и проверка подписи. Алгоритмы ЭЦП.	
			20. Подпись RSA. Подпись DSS. подпись ГОСТ Р 34.10-2001.	

4.	ПК-4	Способность работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности	21. Хэш протакол MD4 и MDC. 22. Хэш протакол MD5 и RIPEMD.	

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать: *(ПК-2)* - приемы самостоятельного изучения криптографических методов; - анализ сильных и слабых мест в используемых алгоритмах. *(ПК-3)* - сильные и слабые стороны используемого алгоритма. *(ПК-4)* - источники формирования информационной базы, характеризующей функционирование экономических систем в сфере международной торговли и внешнеэкономических связей; **Уметь:** *(ПК-2)* - выбрать подходящий алгоритм для заданной задачи. *(ПК-3)* - самостоятельно выбирать методы и приемы при решении криптографических, математических и логических задач; *(ПК-4)* - использовать источники экономической, социальной, управленческой информации для анализа экономических процессов, выявления проблем и определения способов их решения. **Владеть:** *(ПК-2)* - навыками решения задач из разных областей криптографии; *(ПК-3)* - приемами анализа результатов решения и сопоставления с конкретной ситуацией. *(ПК-4)* - навыками сбора, анализа и обработки данных для решения	**Отлично**	Демонстрирует четкое представление, готовность к адекватному применению методов и свойств вычислений, применяемых в криптографии. Может применять все основные показатели и объяснять все основные проблемы стойкости криптосистем. Может применять методы решения основных криптографических задач. Демонстрирует четкое представление о сложности выполнения основных криптографических примитивов Может применять методы криптографии при решении задач защиты информации Может осуществлять программную реализацию криптографических алгоритмов с применением только специализированных средств Демонстрирует четкое умение проводить анализ стойкости криптосистем
	Хорошо	Допускает неточности (понимает сущность) методов и свойств вычислений, применяемых в криптографии Может применять некоторые показатели и объяснять проблемы стойкости криптосистем Может применять методы решения некоторых криптографических задач Допускает неточности (понимает сущность) сложности выполнения основных криптографических примитивов. Может применять методы криптографии при решении задач некоторых защиты информации Может осуществлять программную

текущих и стратегических внешнеэкономических задач.		реализацию криптографических алгоритмов с применением только базовых языковых средств. Осознает значимость стойкости криптосистем
	Удовлетворительно	Имеет фрагментарное представление о методах и свойствах вычислений, применяемых в криптографии Демонстрирует слабое владение показателями и проблемами стойкости криптосистем, а также методами решения основных криптографических задач Имеет неполное представление о сложности выполнения основных криптографических примитивов Демонстрирует слабое умение применять методы криптографии при решении задач защиты информации и осуществлять программную реализацию криптографических алгоритмов
	Неудовлетворительно	Не имеет представление о методах и свойствах вычислений, применяемых в криптографии Демонстрирует большинство показателей на недостаточном и крайне низком уровне.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Дисциплина Криптографические методы защиты информации направлена на ознакомление обучающихся с местом и ролью криптографии в современном мире, мировой культуре и истории; на получение теоретических знаний и практических навыков применения системы шифрования для обеспечения собственной информационной защиты и решения технологических проблем на бедующем месте работы, а также осуществления поиска, хранения, обработки и анализа информации из различных источников и представления ее в соответствующем виде и для их дальнейшего использования в практической деятельности.

Изучение данной дисциплины предусматривает:

- лекции,
- лабораторные работы;
- контрольную работу;
- экзамен;
- самостоятельную работу студента.

Для фиксирования успешности обучения предусматривается экзамен.

В ходе освоения разделов дисциплины студенты должны уяснить идеи и принципы криптографии, ее роль и место в мире, а так же практическую значимость как для одного человека, так и для целого государства. Студенты осваивают основные приемы и методы построения и анализа простых и средних по сложности алгоритмов шифрования.

Студентам необходимо овладеть навыками и умениями применения изученных методов для разработки и реализации профессионально ориентированных проектов в последующей учебной деятельности.

Овладение ключевыми понятиями является основой усвоения учебного материала по дисциплине.

При подготовке к экзамену особое внимание необходимо уделить рекомендациям и замечаниям преподавателей, ведущих аудиторные занятия по дисциплине

В процессе проведения лабораторных занятий происходит закрепление знаний, формирование умений и навыков применения различных методов решения различных алгоритмов шифрования.

Самостоятельную работу необходимо начинать с чтения лекций и учебников.

В процессе консультации с преподавателем обучающийся выясняет наличие пробелов в знаниях и способах решения разных ситуаций.

Работа с литературой является важнейшим элементом в получении знаний по дисциплине. Прежде всего, необходимо воспользоваться списком рекомендуемой по данной дисциплине литературой. Дополнительные сведения по изучаемым темам можно найти в периодической печати и Интернете.

Предусмотрено проведение аудиторных занятий в виде презентаций для наглядного представления и ситуаций общения.

Приложение 2

АННОТАЦИЯ
рабочей программы дисциплины
Криптографические методы защиты информации

1. Цель и задачи дисциплины

Целью изучения дисциплины является: ознакомление студентов с математическими основами современной криптографии, принципами защиты информации с помощью криптографических методов и способов реализации этих методов на практике. Знакомит обучающегося с ролью криптографии в современном мире, мировой культуре и истории.

Задачи дисциплины состоят в том, чтобы освоить студентом основ системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов синтеза и анализа шифров; математических методов, используемых в криптоанализе.

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: Лк.-17 час., ЛР-51 час.; СР-31 час.

Общая трудоемкость дисциплины составляет 144 часа, 4 зачетных единиц

2.2 Основные разделы дисциплины:

1 - Введение в криптографию. Математические операции в криптографии.
2 - Системы шифрования.
3 - Хеш-функции.

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-2 - Способность понимать, совершенствовать и применять математический аппарат.
ПК-3 - Способность критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности.
ПК-4 - Способность работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности.

4. Виды промежуточной аттестации: экзамен

Приложение 3

Протокол о дополнениях и изменениях в рабочей программе
на 20___-20___ учебный год

1. В рабочую программу по дисциплине вносятся следующие дополнения:
_____
_____

2. В рабочую программу по дисциплине вносятся следующие изменения:

_____
_____
_____

Протокол заседания кафедры №____ от «___» _____ 20 ____ г.,
(разработчик)

Заведующий кафедрой _____ _____
(подпись) *(Ф.И.О.)*

Приложение 4

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт).

№ компе-тенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-2	Способность понимать, совершенствовать и применять математический аппарат	**1.** Введение в криптографию. Математические операции в криптографии	1.1 Введение в криптографию	ЛР, кр
			1.2 Шифры	ЛР, кр
			1.3 Математические операции в криптографии	ЛР, кр
ПК-3	Способность критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности	**2.** Системы шифрования	2.1 Системы симметричного шифрования	ЛР, кр
			2.2 Системы асимметричного шифрования	ЛР, кр
		3. Хеш-функции	3.1 Понятие Хеш-функции	ЛР, кр
ПК-4	Способность работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности		3.2 Цифровая подпись.	ЛР, кр

2. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать: *(ПК-2)* - приемы самостоятельного изучения криптографических методов; - анализ сильных и слабых мест в используемых алгоритмах. *(ПК-3)* - сильные и слабые стороны используемого алгоритма. *(ПК-4)* - источники формирования информационной базы, характеризующей функционирование экономических систем в сфере международной торговли и внешнеэкономических связей; **Уметь:** *(ПК-2)* - выбрать подходящий алгоритм для заданной задачи. *(ПК-3)* - самостоятельно выбирать методы и приемы при решении криптографических, математических и логических задач; *(ПК-4)* - использовать источники экономической, социальной, управленческой информации для анализа экономических процессов, выявления проблем и определения способов их решения. **Владеть:** *(ПК-2)* - навыками решения задач из разных областей криптографии; *(ПК-3)* - приемами анализа результатов решения и сопоставления с конкретной ситуацией. *(ПК-4)* - навыками сбора, анализа и обработки данных для решения текущих и стратегических внешнеэкономических задач.	**Отлично**	Демонстрирует все показатели компетенций на высоком уровне. Знает ключевые понятия криптографии. Умеет выбирать подходящий алгоритм для заданной задачи, а так же воспроизводить его. Владеет методологией и навыками оценки надежности типовых криптографических алгоритмов использованных на объекте информационной безопасности.
	Хорошо	Демонстрирует 75% и более показателей на достаточном и высоком уровне. Знает ключевые понятия криптографии. Умеет выбирать подходящий алгоритм для заданной задачи, а так же воспроизводить его.
	Удовлетворительно	Демонстрирует 50% и более показателей на достаточном уровне.
	Неудовлетворительно	Демонстрирует большинство показателей на недостаточном и крайне низком уровне.

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.02 Прикладная математика и информатика от «12» марта 2015 г. №228

для набора 2015 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «13» июля 2015 г. №475

для набора 2016 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06»июня 2016 г. №429

для набора 2017 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06» марта 2017 г. №125

для набора 2018 года и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «12» марта 2018 г. №130

Программу составил:

Сташок О.В. к.т.н, доцент каф. Математики и физики _____

Рабочая программа рассмотрена и утверждена на заседании кафедры математики и физики

от «21» ноября 2018 г., протокол № 3

Заведующий кафедрой
Математики и физики _____ О.И.Медведева

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой МиФ _____ О.И Медведева

Директор библиотеки _____ Т.Ф.Сотник

Рабочая программа одобрена методической комиссией ЕН факультета

от «20» декабря 2018 г., протокол № 4
Председатель методической комиссии факультета _____ М.А. Варданян

СОГЛАСОВАНО:
Начальник
учебно-методического управления _____ Г.П. Нежевец

Регистрационный №_____

(методический отдел)