МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Благовещенский государственный педагогический университет»

ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
Рабочая программа дисциплины

УТВЕРЖДАЮ
И.о. декана физико-математического факультета ФГБОУ ВО «БГПУ»

_____ **О.А.Днепровская**
«22» мая 2019 г.

Рабочая программа дисциплины
ОСНОВЫ КРИПТОГРАФИИ

Направление подготовки

02.03.03 – МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ И АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Профиль

ТЕХНОЛОГИЯ ПРОГРАММИРОВАНИЯ

Уровень высшего образования
БАКАЛАВРИАТ

Принята
на заседании кафедры физического
и математического образования
(протокол № 9 от «15» мая 2019 г.)

Благовещенск 2019

СОДЕРЖАНИЕ

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Цель дисциплины: обучение студентов, специализирующихся в области информационных систем, основам криптографии, позиционированию общематематических подходов к информационным технологиям, а также применению полученных знаний и навыков к решению ряда профессиональных задач.

1.2 Место дисциплины в структуре ООП: Дисциплина «Основы криптографии» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б1 (Б.1. В.ДВ.01.01). Преподавание дисциплины связано с другими дисциплинами учебного плана: «Алгебра и теория чисел», «Математический анализ».

1.3 Дисциплина направлена на формирование следующих компетенций: ОПК-2, ПК-8:

- **ОПК-2**. Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности, **индикаторами** достижения которой является:

- ОПК-2.1 - **знает:** математические основы программирования и языков программирования, организации баз данных и компьютерного моделирования; математические методы оценки качества, надежности и эффективности программных продуктов; математические методы организации информационной безопасности при разработке и эксплуатации программных продуктов и программных комплексов;
- ОПК-2.2 **– умеет:** использовать этот аппарат в профессиональной деятельности;
- ОПК-2.3 **– имеет навыки:** применения данного математического аппарата при решении конкретных задач.

- ПК-8. Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования.

- ПК-8.1. Знает современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования.
- ПК-8.2. Умеет разрабатывать и реализовывать алгоритмы математических моделей на базе языков и пакетов прикладных программ моделирования.
- ПК-8.3. Имеет практический опыт разработки и реализации алгоритмов их на базе языков и пакетов прикладных программ моделирования.

1.4 Перечень планируемых результатов обучения.

В результате изучения дисциплины студент должен

знать:

- Основные криптосистемы;
- Математическое обоснование криптографии.

уметь:

- применять криптосистему Хилла;
- применять криптосистему Меркля-Хелмана;
- применять криптосистему Месси-Омуры;
- применять криптосистему Диффи-Хелмана;
- применять криптосистему DES;
- применять криптосистему ГОСТ 28147-89.

владеть:

– навыками практического использования аппарата дисциплины при решении конкретных задач.

1.5 Общая трудоемкость дисциплины «Основы криптографии» составляет 3 зачетные единицы (далее – ЗЕ) (108 часов):

Программа предусматривает изучение материала на лекциях и лабораторных занятиях. Предусмотрена самостоятельная работа студентов по темам и разделам. Проверка знаний осуществляется фронтально, индивидуально.

1.6 Объем дисциплины и виды учебной деятельности

Объем дисциплины и виды учебной деятельности (очная форма обучения)

Вид учебной работы	Всего часов	Семестр
		5
Общая трудоемкость	108	108
Аудиторные занятия	60	60
Лекции	24	24
Практические занятия	36	36
Самостоятельная работа	48	48
Вид итогового контроля:		зачет

2 УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

2.1 Очная форма обучения

Учебно-тематический план

Наименование разделов и темы	Всего часов	Виды учебных занятий		
		Лекции	Практические	Самостоятельная работа
Тема1. Основные понятия криптографии.	6	2	2	2
Тема 2. Простейшие методы шифрования с закрытым ключом. Криптосистема Хилла.	14	4	4	6
Тема 3. «Рюкзачная» криптосистема Меркля-Хеллмана	16	4	6	6
Тема 4. Криптосистема «навешивания замков» Месси - Омуры	16	4	4	8
Тема 5. Криптосистема Диффи-Хеллмана.	12	2	4	6
Тема 6. Криптосистема на конечных полях.	12	2	4	6
Тема 7. Криптосистемы DES	12	2	4	6
Тема 8. Криптосистема ГОСТ 28147-89	10	2	4	4

Тема 9. Поточные шифры и генераторы псевдослучайных чисел.	10	2	4	4
Всего:	108	24	36	48

Интерактивное обучение по дисциплине

Тема	Интерактивные формы занятий	Количество часов
Тема 2. Простейшие методы шифрования с закрытым ключом. Криптосистема Хилла.	работа в малых группах	2
Тема 3. «Рюкзачная» криптосистема Меркля-Хеллмана	работа в малых группах	2
Тема 4. Криптосистема «навешивания замков» Месси - Омуры	работа в малых группах	2
Тема 5. Криптосистема Диффи-Хеллмана	работа в малых группах	2
Тема 6. Криптосистема на конечных полях	работа в малых группах	2
ВСЕГО		10

3 СОДЕРЖАНИЕ ТЕМ (РАЗДЕЛОВ)

Тема1. Основные понятия криптографии.

Предмет и задачи криптографии. Основные определения. Требования к криптографическим системам защиты информации. Реализация криптографических методов. Сведения из истории криптографии. Бинарное дерево Морзе. Криптографические атаки. Пример шифра.

Тема 2. Простейшие методы шифрования с закрытым ключом

Общая схема симметричного шифрования. Методы замены. Одноалфавитная замена. Криптосистема Хилла. Шифрование. Расшифрование. Атака на систему.

Тема 3. «Рюкзачная» криптосистема Меркля-Хеллмана

Задача об укладке рюкзака. Представление натурального числа суммой натуральных чисел. Рюкзачный набор. Свойство сверхрастущего набора. Нахождение обратного элемента в модулярной группе. Шифрование. Расшифрование. Атака на систему.

Тема 4. Криптосистема «навешивания замков» Месси - Омуры

Остаток от степени по модулю. «Навешивание замка» как возведение в степень. Обратный элемент в модулярной группе. Шифрование. Расшифрование. Атака на систему.

Тема 5. Криптосистема Диффи-Хеллмана

Дискретное логарифмирование в полях Галуа. Открытый и закрытый клчи. Шифрование. Расшифрование. Атака на систему. Электронная подпись.

Тема 6. Криптосистема на конечных полях

Конечное поле. Неприводимые многочлены. Схема Яковкина. Структура мультипликативной группы поля. Обратный элемент. Шифрование. Расшифрование. Атака на систему.

Тема 7. Криптосистемы DES

Перемешивание и рассеяние элементов блока с помощью таблиц. Переход между блоками. Шифрование. Расшифрование. Атака на систему.

Тема 8. Криптосистема ГОСТ 28147-89

Эллиптические кривые. Операция сложения точек эллиптической кривой. Шифрование. Расшифрование. Атака на систему.

Тема 9. Поточные шифры и генераторы псевдослучайных чисел.

Генераторы псевдослучайных чисел на основе сдвиговых регистров с обратной связью. Использование режимов OFB и CTR блочных шифров для получения псевдослучайных чисел. Алгоритм RC4. Генераторы настоящих случайных чисел в криптографии. Управление секретными ключами. Шифрование. Расшифрование. Атака на систему.

4 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ (УКАЗАНИЯ) ДЛЯ СТУДЕНТОВ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ

4.1 Общие методические рекомендации

Рабочая программа дисциплины призвана помочь студентам физико-математического факультета в организации самостоятельной работы по освоению дисциплины «Основы криптографии».

Согласно учебному плану организация учебной деятельности по дисциплине «Основы криптографии» предусматривает следующие формы: лекция, практические занятия. В содержании дисциплины большое внимание уделено новым направлениям криптографии, связанным с обеспечением конфиденциальности взаимодействия пользователей компьютеров и компьютерных сетей. Рассмотрены основные широко используемые блочные и поточные шифры, шифры с открытым ключом и методы цифровой (электронной) подписи. Уделено внимание отечественным государственным стандартам в области криптографической защиты информации.

4.2 Методические рекомендации по подготовке к лекциям

Курс лекций строится на основе четких понятий и формулировок, так как только при таком походе студенты приобретают культуру абстрактного мышления, необходимую для высококвалифицированного специалиста в любой отрасли знаний, а также на разборе типовых задач и алгоритмов их решения.

4.3 Методические рекомендации по подготовке к практическим занятиям

При подготовке к практическим занятиям студент должен просмотреть конспекты лекций, рекомендованную литературу по данной теме; подготовиться к ответам на контрольные вопросы.

4.4 Методические указания к самостоятельной работе студентов

В теме 1. Основные понятия криптографии определяются предмет и задачи криптографии, формулируются основополагающие определения курса и требования к криптографическим системам защиты информации, дается историческая справка об основных этапах развития криптографии как науки. Также рассматривается пример простейшего шифра, на основе которого поясняются сформулированные понятия и тезисы. В теме 2. Простейшие методы

шифрования с закрытым ключом рассматривается общая схема симметричного шифрования, а также дается классификация простейших методов симметричного шифрования. Описание каждого из указанных в классификации шифров сопровождается примером. Следует обратить внимание на нахождение обратной матрицы в криптосистеме Хилла.
В теме 3. «Рюкзачная» криптосистема Меркля-Хеллмана следует обратить внимание на задачу «о рюкзаке», свойство сверхрастущего набора. В теме 4. Криптосистема «навешивания замков» Месси – Омуры следует обратить внимание на нахождение остатка от степени по модулю, операции «навешивания замка» как возведение в степень. В теме 5. Криптосистема Диффи-Хеллмана следует обратить внимание на дискретное логарифмирование в полях Галуа. В теме 6. Криптосистема на конечных полях следует обратить внимание на квадратичное расширение поля. Быстрое возведение в степень. Символы Лежандра и Якоби. В теме 7. Криптосистемы DES следует обратить внимание на понятия перемешивание и рассеяние элементов блока с помощью таблиц, переход между блоками. В теме 8. Криптосистемы ГОСТ 28147-89 следует обратить внимание на понятия перемешивание и рассеяние элементов блока с помощью таблиц, переход между блоками. В теме 9. Поточные шифры и генераторы псевдослучайных чисел. можно узнать, каким образом производится шифрование при передаче данных в режиме реального времени. Сформулированы принципы использования генераторов псевдослучайных ключей при потоковом шифровании. Рассматриваются некоторые простейшие генераторы псевдослучайных чисел: линейный конгруэнтный, генератор по методу Фибоначчи с запаздыванием, генератор псевдослучайных чисел на основе алгоритма BBS. Описание каждого из алгоритмов сопровождается примером, в котором поясняются особенности использования того или иного метода генерации псевдослучайных чисел.

4.5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине:

1. Фонд оценочных средств.
2. Список литературы и информационных ресурсов.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Наименование раздела (темы) дисциплины	Формы/виды самостоятельной работы	Количество часов, в соответствии с учебно-тематическим планом
Тема1. Основные понятия криптографии	Подготовка к индивидуальному заданию. Выполнение индивидуального задания	2
Тема 2. Простейшие методы шифрования с закрытым ключом	Подготовка к индивидуальному заданию. Выполнение индивидуального задания	6
Тема 3. «Рюкзачная» криптосистема Меркля-Хеллмана	Подготовка к индивидуальному заданию. Выполнение индивидуального задания	6

Тема 4. Криптосистема «навешивания замков» Месси - Омуры	Подготовка к индивидуальному заданию. Выполнение индивидуального задания	8
Тема 5. Криптосистема Диффи-Хелл-мана	Подготовка к индивидуальному заданию. Выполнение индивидуального задания	6
Тема 6. Криптосистема на конечных полях	Подготовка к индивидуальному заданию. Выполнение индивидуального задания	6
Тема 7. Криптосистемы DES	Подготовка к индивидуальному заданию. Выполнение индивидуального задания	6
Тема 8. Криптосистема ГОСТ 28147-89	Подготовка к индивидуальному заданию. Выполнение индивидуального задания	4
Тема 9. Поточные шифры и генераторы псевдослучайных чисел.	Подготовка к индивидуальному заданию. Выполнение индивидуального задания	4
Итого		48

5 ПРАКТИКУМ ПО ДИСЦИПЛИНЕ

.

Практическое занятие №1 (2 часа)

Тема1. Основные понятия криптографии.

Предмет и задачи криптографии. Основные определения. Требования к криптографическим системам защиты информации. Реализация криптографических методов. Сведения из истории криптографии. Бинарное дерево Морзе. Криптографические атаки. Пример шифра

Задания размещены в СЭО БГПУ.

Литература

1. Введение в криптографию: Базовый курс для студ. математич. спец. вузов / ред. В. В. Ященко. – 3-е изд. – М. ; Харьков ; Минск; СПб. : Питер, 2001. – 287 с.
2. Введение в теоретико-числовые методы криптографии : учеб. пособие для студ. вузов / М. М. Глухов [и др.]. – СПб. ; М. ; Краснодар : Лань, 2011. - 394 с. – **ISBN** 978-5-8114-1116-0 10 экз.
3. Осипян, В.О. Криптография в задачах и упражнениях / В.О. Осипян, К.В. Осипян – М.: Гелиос АРВ, 2004

Практическое занятие № 2,3 (4 часа)

Тема 2. Простейшие методы шифрования с закрытым ключом

Общая схема симметричного шифрования. Методы замены. Одноалфавитная замена. Криптосистема Хилла. Шифрование. Расшифрование. Атака на систему.

Задания размещены в СЭО БГПУ.

Литература

1. Введение в криптографию: Базовый курс для студ. математич. спец. вузов / ред. В. В. Ященко. - 3-е изд. - М. ; Харьков ; Минск; СПб. : Питер, 2001. - 287 с.
2. Смолин, Ю.Н. Алгебра и теория чисел: учеб. пособие для студ.вузов / Ю.Н. Смолин. – М.: Флинта: Наука, 2006. – 463 с.
3. http://www.intuit.ru/studies/courses/691/547/literature Основы криптографии

Практическое занятие № 4,5,6 (6 часов)

Тема 3. «Рюкзачная» криптосистема Меркля-Хеллмана

Задача об укладке рюкзака. Представление натурального числа суммой натуральных чисел. Рюкзачный набор. Свойство сверхрастущего набора. Нахождение обратного элемента в модулярной группе. Шифрование. Расшифрование. Атака на систему.

Задания размещены в СЭО БГПУ.

Литература

1. Маховенко, Елена Борисовна. Теоретико-числовые методы в криптографии : учеб. пособие для студ. вузов / Е. Б. Маховенко. – М.: Гелиос АРВ, 2006. – 318, [1] с.
2. Введение в теоретико-числовые методы криптографии : учеб. пособие для студ. вузов / М. М. Глухов [и др.]. – СПб. ; М. ; Краснодар : Лань, 2011. – 394 с. – **ISBN** 978-5-8114-1116-0 10 экз.

Практическое занятие № 7,8 (4 часа)

Тема 4. Криптосистема «навешивания замков» Месси - Омуры

Остаток от степени по модулю. «Навешивание замка» как возведение в степень. Обратный элемент в модулярной группе. Шифрование. Расшифрование. Атака на систему.

Задания размещены в СЭО БГПУ.

Литература

1. Осипян, В.О. Криптография в задачах и упражнениях / В.О. Осипян, К.В. Осипян – М.: Гелиос АРВ, 2004
2. Элементы криптографии. Основы теории защиты информации / Нечаев В.И. – М.: Высш. шк., 1999. – 108 с.
3. http://alexinternetclic.ru/Kriptograf.php Современные подходы к построению криптографических методов

Практическое занятие № 9, 10 (4 часа)

Тема 5. Криптосистема Диффи-Хеллмана

Дискретное логарифмирование в полях Галуа. Открытый и закрытый ключи. Шифрование. Расшифрование. Атака на систему. Электронная подпись.

Задания размещены в СЭО БГПУ.

Литература

1. Введение в криптографию: Базовый курс для студ. математич. спец. вузов / ред. В. В. Ященко. – 3-е изд. – М. ; Харьков ; Минск; СПб. : Питер, 2001. – 287 с.

2. Введение в теоретико-числовые методы криптографии : учеб. пособие для студ. вузов / М. М. Глухов [и др.]. – СПб. ; М. ; Краснодар : Лань, 2011. – 394 с. – **ISBN** 978-5-8114-1116-0 10 экз.
3. Осипян, В.О. Криптография в задачах и упражнениях / В.О. Осипян, К.В. Осипян – М.: Гелиос АРВ, 2004

Практическое занятие № 11, 12 (4 часа)

Тема 6. Криптосистема на конечных полях

Конечное поле. Неприводимые многочлены. Схема Яковкина. Структура мультипликативной группы поля. Обратный элемент. Шифрование. Расшифрование. Атака на систему.

Задания размещены в СЭО БГПУ.

Литература

1. Введение в криптографию: Базовый курс для студ. математич. спец. вузов / ред. В. В. Ященко. - 3-е изд. - М. ; Харьков ; Минск; СПб. : Питер, 2001. - 287 с.
2. Смолин, Ю.Н. Алгебра и теория чисел: учеб. пособие для студ.вузов / Ю.Н. Смолин. – М.: Флинта: Наука, 2006. – 463 с.
3. Вернер, М. Основы кодирования: Пер. с нем. / М. Вернер. – М.: ТЕХНОСФЕРА, 2004. – 288 с.
4. Золотарев, В.В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. / В.В. Золотарев, Г.В. Овечкин – М.: Горячая линия – Телеком, 2004. – 126 с.

Практическое занятие №13, 14 (4 часа)

Тема 7. Криптосистемы DES

Перемешивание и рассеяние элементов блока с помощью таблиц. Переход между блоками. Шифрование. Расшифрование. Атака на систему.

Задания размещены в СЭО БГПУ.

Литература

1. http://alexinternetclic.ru/Kriptograf.php Современные подходы к построению криптографических методов
2. http://www.intuit.ru/studies/courses/691/547/literature Основы криптографии

Практическое занятие № 15, 16 (4 часа)

Тема 8. Криптосистема ГОСТ 28147-89

Эллиптические кривые. Операция сложения точек эллиптической кривой. Шифрование. Расшифрование. Атака на систему.

Задания размещены в СЭО БГПУ.

Литература

1. Элементы криптографии. Основы теории защиты информации / Нечаев В.И. – М.: Высш. шк., 1999. – 108 с.
2. http://alexinternetclic.ru/Kriptograf.php Современные подходы к построению криптографических методов
3. http://www.intuit.ru/studies/courses/691/547/literature Основы криптографии

Практическое занятие №17, 18 (4 часа)

Тема 9. Поточные шифры и генераторы псевдослучайных чисел.
Генераторы псевдослучайных чисел на основе сдвиговых регистров с обратной связью. Использование режимов OFB и CTR блочных шифров для получения псевдослучайных чисел. Алгоритм RC4. Генераторы настоящих случайных чисел в криптографии.
Управление секретными ключами. Шифрование. Расшифрование. Атака на систему.

Задания размещены в СЭО БГПУ.

Литература

1. Золотарев, В.В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. / В.В. Золотарев, Г.В. Овечкин – М.: Горячая линия – Телеком, 2004. – 126с.
2. Элементы криптографии. Основы теории защиты информации / Нечаев В.И. – М.: Высш. шк., 1999. – 108 с.
3. http://alexinternetclic.ru/Kriptograf.php Современные подходы к построению криптографических методов

6 ДИДАКТИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ КОНТРОЛЯ (САМОКОНТРОЛЯ) УСВОЕННОГО МАТЕРИАЛА

6.1 Оценочные средства, показатели и критерии оценивания компетенций

Индекс компетенции	Оценочное средство	Показатели оценивания	Критерии оценивания сформированности компетенций
ОПК-2	индивидуальное задание	Низкий (не зачтено)	задания, размещенные в Электронной информационно-образовательной среде БГПУ выполнены менее чем на 60 процентов
		Пороговый (зачтено)	задания, размещенные в Электронной информационно-образовательной среде БГПУ выполнены на 60 и более процентов

6.2 Промежуточная аттестация студентов по дисциплине

Промежуточная аттестация является проверкой всех знаний, навыков и умений студентов, приобретённых в процессе изучения дисциплины. Формой промежуточной аттестации по дисциплине является зачёт.

Для оценивания результатов освоения дисциплины применяется следующие критерии оценивания.

Критерии оценивания индивидуального задания

Индивидуальное задание студенту засчитывается если: студент, предоставил верно решенное задание разместив его СЭО

Критерии оценивания на зачете

Оценка «зачтено» ставится студенту, если
1) теоретические вопросы индивидуальных заданий изложены полно, математически грамотно, логически верно, без существенных ошибок,
2) показано умение иллюстрировать теоретические положения конкретными примерами,
3) правильно, и грамотно решены задачи, индивидуальных заданиях, может быть при решении допускаются незначительные ошибки,
4) продемонстрирована сформированность компетенций.

Оценка «не зачтено» ставится, если студент
1) не раскрыл основное содержание теоретического материала, не расшифровал большую часть текста,
2) или показывает незнание или непонимание наиболее важной части учебного теоретического материала,
3) или допущены ошибки в изложении теоретических вопросов, и они не исправлены после нескольких наводящих вопросов,
4) не сформированы компетенции,

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения дисциплины

Индивидуальное задание **№1.**

Составить по ключевому слову матрицу Хилла, найти обратную и прочитать шифр

	матрица	Шифр	текст
Вариант 1	сколько ?	уад?ьузэклюзаийбв?н	В этом нет сомнения
Вариант 2	приветики	нёяижсгшгбьойгиюцдз,аааа	когда обрывается лента
Вариант 3	воробейка	ю?яяги, уынфжвш	выгодное дельце
Вариант 4	позвольте	мел,яыэьэщямхдфй,ё	дело о звёздочке
Вариант 5	хлестаков	Пшпимгрбётрьёбёчщс	если дорога жизнь

Индивидуальное задание **№2.**

С использованием кодировки алфавита расшифровать по системе Меркла-Хеллмана

0	пробел	0	0	0	0	0
1	A	0	0	0	0	1
2	B	0	0	0	1	0
3	C	0	0	0	1	1

Вариант 1												
шифр	4945			3860	3619	3399	3775	4988	3291	3478		
рюк-зайный набор	47			141	282	564	1128	2209	1552	661	1322	2127
модуль	2913				держим в тайне							
ключ шифрова-ния				47								
Вариант 2												
шифр	1388			3047	2312	3644	1988	990				
рюк-зайный набор	33			66	132	297	561	1155	430	827	104	1758
модуль	1913				держим в тайне							
ключ шифрова-ния				33								
Вариант 3												
шифр	1258			1104	3078	1132	1740					
рюк-зайный набор	29			58	145	261	551	1131	291	553	1251	502
модуль	1942				держим в тайне							
ключ шифрова-ния				29								
Вариант 4												
шифр	4336			1774	2019	622	2556	2641	216			
рюк-зайный набор	36			72	180	396	756	1548	289	974	1552	333
модуль	2771				держим в тайне							
ключ шифрова-ния				36								

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ 3

С использованием кодировки алфавита расшифровать по системе «навешивания замков» Месси - Омуры

Вариант1.									
модуль	167								
ключ шифрования 1	17								
ключ шифрования 2	19								
щифр	120	19	1	16	52	150			
Вариант 2.									
модуль	257								
ключ шифрования 1	23								
ключ шифрования 2	5								
щифр	193	140	143	237	96				
Вариант 3.									
модуль	347								
ключ шифрования 1	7								
ключ шифрования 2	17								
щифр	298	50	280	1	268	241			
Вариант 4.									
модуль	211								
ключ шифрования 1	23								
ключ шифрования 2	13								
щифр	24	143	21	36	48	196			
Вариант 5.									
модуль	173								
ключ шифрования 1	5								
ключ шифрования 2	3								
щифр	23	78	123	19	70	1	62	159	

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ 4

С использованием кодировки алфавита расшифровать по криптосистеме Диффи- Хелл-мана

1.								
модуль	209							
ключ шифрования l	13							
щифр	160	25	189	25	192	178		
2.								
модуль	95							
ключ шифрования l	7							
щифр	2	71	88	20	71	37		
3.								
модуль	391							
ключ шифрования l	9							
щифр	62	83	35	235	144	83	343	80
4.								
модуль	851							
ключ шифрования l	5							
щифр	1	144	144	1	348	572	340	
5.								
модуль	667							
ключ шифрования l	9							
щифр	149	90	107	288	1	183	149	288

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ 5

Задания на крипосистему Эль Гамаля

1.									
модуль	47251								
секретный ключ x	7525								
первообразный корень g	10								
сессионный ключ k	9								
щифр	a	27087	27087	27087	27087	27087	27087	27087	27087
	b	20466	24380	503	10233	20969	30699	3914	503

2.									
модуль	51853								
секретный ключ x	1131								
первообразный корень g	11								
сессионный ключ k	19								
щифр	a	16928	16928	16928	16928	16928	16928	16928	16928
	b	7441	37205	156	15038	22323	156	234	37205
3.									
модуль	63691								
секретный ключ x	54771								
первообразный корень g	15								
сессионный ключ k	23								
щифр	a	23375	23375	23375	23375	23375	23375	23375	23375
	b	23526	21088	16212	49490	42176	61253	53939	61253
4.									
модуль	46489								
секретный ключ x	25778								
первообразный корень g	29								
сессионный ключ k	13								
щифр	a	5240	5240	5240	5240	5240	5240	5240	5240
	b	780	975	585	3510	975	195	3705	975
5.									
модуль	48649								
секретный ключ x	10727								
первообразный корень g	7								
сессионный ключ k	17								
щифр	a	41425	41425	41425	41425	41425	41425	41425	41425
	b	30267	28524	23770	21393	30267	39775	634	39775

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ 6

Расшифровать по криптосистеме DES

Вариант 1

1	0	1	0	0	1	1	0
1	0	1	1	1	1	0	0
0	1	0	0	0	0	1	1
0	1	1	0	1	1	0	1
0	1	1	1	0	0	0	1
0	0	1	0	0	1	1	0
1	0	0	1	0	1	1	0
0	0	0	1	0	0	1	0

Вариант 2

1	0	1	0	0	0	1	0
1	0	1	0	0	0	1	0
0	1	0	0	0	1	0	1
0	1	1	0	1	1	1	0
1	1	1	0	0	0	0	1
0	0	1	0	1	1	1	1
1	0	0	0	1	1	0	0
1	0	0	1	1	0	0	1

Вариант 3

1	1	0	0	1	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	1	0	0	0
0	1	1	1	0	1	1	0
0	0	0	1	0	0	1	0

1	1	0	0	0	1	1	0
0	0	1	1	1	0	1	0
0	1	0	1	0	0	0	1

1.

0	0	0	0	0	1	1	0
1	0	0	1	0	0	0	0
0	1	0	0	1	0	0	0
0	0	1	1	0	1	1	0
1	1	0	0	1	0	1	0
1	0	0	0	1	1	1	0
0	1	0	0	1	0	1	1
1	1	1	0	1	0	1	1

2.

1	0	1	1	1	1	0	0
1	0	1	0	1	1	0	1
0	1	0	0	0	0	1	0
0	1	1	0	0	1	0	0
1	0	0	0	0	0	0	0
1	1	0	1	1	1	0	0
0	1	0	1	0	1	1	1
1	0	0	0	1	0	0	1

3.

1	1	1	1	0	0	0	0
0	0	1	1	0	0	1	0
0	1	0	0	0	0	0	1

0	1	1	1	0	1	0	0
0	0	1	1	1	1	1	0
0	0	1	0	1	1	0	1
1	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1

4.

0	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0
0	0	1	0	0	1	0	1
0	0	0	1	1	0	1	1
0	0	0	1	0	0	1	1
1	1	1	1	1	1	0	0
1	1	0	0	1	0	1	1
1	1	0	1	0	0	0	0

5.

1	0	0	1	1	1	0	0
0	0	0	1	1	0	0	0
0	0	1	0	1	0	0	0
0	0	0	1	0	0	0	1
0	0	1	1	1	0	1	0
1	0	1	1	0	1	1	0
1	0	1	0	1	0	1	0
1	0	0	1	0	1	1	0

6.3.2 Программа зачета

1 Предмет и задачи криптографии. Основные определения. Требования к криптографическим системам защиты информации.

2 Сведения из истории криптографии.

3 Бинарное дерево Морзе.

4 Криптосистема Хилла.

5 «Рюкзачная» криптосистема Меркля-Хеллмана. Задача об укладке рюкзака. Представление натурального числа суммой натуральных чисел. Рюкзачный набор. Свойство сверхрастущего набора. Нахождение обратного элемента в модулярной группе.

6 Криптосистема «навешивания замков» Месси - Омуры. Остаток от степени по модулю. «Навешивание замка» как возведение в степень. Обратный элемент в модулярной группе.

7 Криптосистема Диффи-Хеллмана. Дискретное логарифмирование в полях Галуа. Открытый и закрытый ключи. Электронная подпись.

8 Криптосистема Уильямса. Квадратичное расширение поля. Быстрое возведение в степень. Символы Лежандра и Якоби.

9 Криптосистемы DES, ГОСТ 28147-89. Перемешивание и рассеяние элементов блока с помощью таблиц. Переход между блоками.

10 Поточные шифры и генераторы псевдослучайных чисел. Генераторы псевдослучайных чисел на основе сдвиговых регистров с обратной связью.

7 ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ В ПРОЦЕССЕ ОБУЧЕНИЯ

Информационные технологии – обучение в электронной образовательной среде с целью расширения доступа к образовательным ресурсам, увеличения контактного взаимодействия с преподавателем, построения индивидуальных траекторий подготовки, объективного контроля и мониторинга знаний студентов.

В образовательном процессе по дисциплине используются следующие информационные технологии, являющиеся компонентами Электронной информационно-образовательной среды БГПУ:

- Официальный сайт БГПУ;
- Корпоративная сеть БГПУ;
- Система электронного обучения ФГБОУ ВО «БГПУ»;
- Электронные библиотечные системы;
- Мультимедийное сопровождение лекций и практических занятий.

8 ОСОБЕННОСТИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ ИНВАЛИДАМИ И ЛИЦАМИ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

При обучении лиц с ограниченными возможностями здоровья применяются адаптивные образовательные технологии в соответствии с условиями, изложенными в раздел «Особенности организации образовательного процесса по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья» основной образовательной программы (использование специальных учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь и т.п.) с учётом индивидуальных особенностей обучающихся.

9 СПИСОК ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

9.1 Литература

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. – Москва : Издательство Юрайт, 2022. – 349 с. – (Высшее образование). – ISBN 978-5-534-02883-6. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/489919 (дата обращения: 10.10.2022).

2. Введение в криптографию: Базовый курс для студ. математич. спец. вузов / ред. В. В. Ященко. – 3-е изд. – М. ; Харьков ; Минск; СПб. : Питер, 2001. – 287 с. (9 экз.)

3. Введение в теоретико-числовые методы криптографии : учеб. пособие для студ. вузов / М. М. Глухов [и др.]. – СПб. ; М. ; Краснодар : Лань, 2011. – 394 с. – **ISBN** 978-5-8114-1116-0 (10 экз.)

4. Нечаев В.И. Элементы криптографии. Основы теории защиты информации / Нечаев В.И. – М. : Высш. шк., 1999. – 108 с. (20 экз.)

5. Молдовян, А.А. Криптография : учеб. пособие / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов. – СПб. : Лань, 2001. – 218 с. (10 экз.)

9.2 Базы данных и информационно-справочные системы

1. Федеральный портал «Российское образование» – Режим доступа : http://www.edu.ru

2. Информационная система «Единое окно доступа к образовательным ресурсам» – Режим доступа : http://www.window.edu.ru

3. Федеральный центр информационно-образовательных ресурсов – Режим доступа : http://fcior.edu.ru

4. Сайт Федеральной службы по интеллектуальной собственности, патентам и товарным знакам (Роспатента). – Режим доступа : http://www.fips.ru/rospatent/index.htm

9.3 Электронно-библиотечные ресурсы

1. ЭБС «Юрайт». – Режим доступа : https://urait.ru
2. Полпред (обзор СМИ). – Режим доступа : https://polpred.com/news

10 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются аудитории, оснащённые учебной мебелью, аудиторной доской в том числе интерактивной, компьютером(рами) с установленным лицензионным специализированным программным обеспечением, коммутатором для выхода в электронно-библиотечную систему и электронную информационно-образовательную среду ФГБОУ ВО «БГПУ», мультимедийными проекторами, экспозиционными экранами, учебно-наглядными пособиями (стенды, таблицы, мультимедийные презентации, видео материалы). Самостоятельная работа студентов организуется в аудиториях оснащенных компьютерной техникой с выходом в электронную информационно-образовательную среду вуза, в специализированных лабораториях по дисциплине, а также в залах доступа в локальную сеть БГПУ, в лаборатории психолого-педагогических исследований и др.

Лицензионное программное обеспечение: операционные системы семейства Windows, Linux; офисные программы Microsoft office, Libreoffice, OpenOffice; Adobe Photoshop, Matlab, DrWeb antivirus, компьютерная программа TMashine и т.д.

Разработчик: Алутин П.П., кандидат физико-математических наук, доцент

11 ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

Утверждение изменений и дополнений в РПД для реализации в 2020/2021 уч. г.

РПД обсуждена и одобрена для реализации в 2020/2021 уч. г. на заседании кафедры физического и математического образования (протокол № 10 от «16» июня 2020 г.). В РПД внесены следующие изменения и дополнения:

№ изменения: 1 № страницы с изменением: Титульный лист	
Исключить:	Включить:
Текст: Министерство науки и высшего образования РФ	Текст: Министерство просвещения Российской Федерации

Утверждение изменений и дополнений в РПД для реализации в 2021/2022 уч. г.

РПД обсуждена и одобрена для реализации в 2021/2022 уч. г. без изменений на заседании кафедры физического и математического образования (протокол №8 от 21.04.2021 г.).

Утверждение изменений и дополнений в РПД для реализации в 2022/2023 уч. г.

РПД пересмотрена, обсуждена и одобрена для реализации в 2022/2023 учебном году на заседании кафедры физического и математического образования (протокол №1 от 21 сентября 2022 г.).

В рабочую программу внесены следующие изменения и дополнения:

№ изменения: 1 № страницы с изменением: 21	
В Раздел 9 внесены изменения в список литературы, в базы данных и информационно-справочные системы, в электронно-библиотечные ресурсы. Указаны ссылки, обеспечивающие доступ обучающимся к электронным учебным изданиям и электронным образовательным ресурсам с сайта ФГБОУ ВО «БГПУ».	