Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кубанский государственный университет»

Факультет компьютерных технологий и прикладной математики Кафедра вычислительных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.28 «Криптографические протоколы»

Направление подготовки/специальность 02.03.02 **Фундаментальная информатика и информационные технологии**
(код и наименование направления подготовки/специальности)

Направленность (профиль) /специализация
Математическое и программное обеспечение компьютерных технологий

Программа подготовки *академический бакалавриат*

Форма обучения *очная*

Квалификация выпускника *бакалавр*

Краснодар 2022

Рабочая программа дисциплины «СОВРЕМЕННЫЕ КОНЦЕПЦИИ ПРОГРАММИРОВАНИЯ» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Программу составил(а):

Жук Арсений Сергеевич, ст. преподаватель
Ф.И.О. , должность, ученая степень, ученое звание — подпись

Рабочая программа дисциплины «СОВРЕМЕННЫЕ КОНЦЕПЦИИ ПРОГРАММИРОВАНИЯ» утверждена на заседании кафедры Вычислительных технологий протокол № 9 «18 » мая 2022 г.

Заведующий кафедрой (разработчика) Вишняков Ю.М

(фамилия, инициалы — подпись

Утверждена на заседании учебно-методической комиссии факультета Компьютерных Технологий и Прикладной Математики
протокол № 6 от «25» мая 2022 г

Председатель УМК факультета Коваленко А.В.

фамилия, инициалы — подпись

Рецензенты:

Гаркуша О.В., доцент кафедры информационных технологий ФБГОУ ВО «Кубанский государственный университет», кандидат физико-математических наук.

Схаляхо Ч.А., доцент КВВУ им.С.М.Штеменко, к.ф.-м.н., доцент

1. Цели и задачи освоения дисциплины

1.1 Цель освоения дисциплины

Учебная дисциплина «Криптографические протоколы» предназначена для профессиональной разработки с применением криптографической защиты.

Целью курса «Криптографические протоколы» является изучение математических основ криптологии, основных криптоалгоритмов, стандартных криптопротоколов и аспектов их применения.

1.2 Задачи дисциплины

В результате освоения данной компетенции студент должен:

знать основные блоки симметричных шифров, математические аспекты безопасности шифров, стандарты и ГОСТы криптопротоколов.

уметь построить программную реализацию существующих криптоалгоритмов средствами произвольного языка, построить криптопротокол обмена информацией с помощью встроенных библиотек, построить модель реализации заданной атаки на криптопротокол;

владеть навыками свободного обращения с программными реализациями криптоалгоритмов; навыками построения архитектуры защищенных программных систем с применением существующих протоколов.

1.3. Место дисциплины (модуля) в структуре образовательной программы

Курс «Криптографические протоколы» относится к части, формируемой участниками образовательных отношений блока Б1 Дисциплины (модули) и является обязательной.

Для изучения дисциплины студент должен владеть знаниями, умениями и навыками по дисциплинам: Алгебра, Дискретная математика, Теория графов и ее приложения, Комбинаторный анализ, Информационная безопасность, Программирование в компьютерных сетях, Интерпретируемые языки программирования, Платформо-независимое программирование, с которыми дисциплина связана логически и содержательно-методически.

Дисциплина является предшествует изучению дисциплин: «Преддипломная практика», «Защита выпускной квалификационной работы».

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих **компетенций:**

Код и наименование индикатора	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ОПК-5 Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	
Формулировки индикаторов	
ОПК-5.1. Знает методику установки и администрирования информационных систем и баз данных. Знаком с содержанием Единого реестра российских программ. ОПК-5.2. Умеет реализовывать техническое сопровождение информационных систем и баз данных.	

Код и наименование индикатора	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ОПК-5.3. Имеет практический опыт участия в научных студенческих конференциях, очных, виртуальных, заочных обсуждениях научных проблем в области информационных технологий.	
ПК-1 Способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания, современные языки программирования и программное обеспечение; операционные системы и сетевые технологии	
Формулировки индикаторов	
ПК-1.1. Знает основы научно- исследовательской деятельности в области информационных технологий, имеет научные знания в теории информационных систем. ПК-1.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности. ПК-1.3. Имеет практический опыт научно- исследовательской деятельности в области информационных технологий.	

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоемкость дисциплины составляет 3 зач.ед. (108 часов), их распределение по видам работ представлено в таблице *(для студентов ОФО)*

Вид учебной работы	Всего часов	Семестры (часы)			
		8			
Контактная работа в том числе:	48,3	48,3			
Аудиторные занятия (всего):	42	42			
В том числе:					
Занятия лекционного типа	14	14			
Занятия семинарского типа (семинары, практ. занятия)					
Лабораторные занятия	28	28			
Иная контрольная работа					
Контроль самостоятельной работы	6	6			
Промежуточная аттестация (ИКР)	0,3	0,3			
Самостоятельная работа (всего)	6	6			
В том числе:					
Курсовая работа					
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий,	2	2			
Подготовка к лабораторным и практическим занятиям.)	2	2			
Подготовка к текущему контролю	2	2			
Контроль:					
Подготовка к экзамену:	53,7	53,7			

Общая трудоемкость	час	108	108			
	в т.ч. контактная работа	48,3	48,3			
	зач. ед.	3	3			

2.1 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины, изучаемые в _8__семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	КСР	ЛР	СРС
1	2	3	4	5	6	7
1	**Раздел 1.** Математические основы криптологии.	20	4		14	2
2	**Раздел 2.** Криптоалгоритмы.	12	4		6	2
3	**Раздел 3.** Криптопротоколы	22	6	6	8	2
	Итого по разделам дисциплины	54	14	6	28	6
	ИКР	0,3				
	Подготовка к экзамену	53,7				53,7
	Итого по дисциплине:	108				

2.2 Содержание разделов дисциплины:
2.2.1 Занятия лекционного типа

№ раз-дела	Наименование раздела	Содержание раздела	Форма текущего контроля	Разработано с участием представителей работодателей
1	2	3	4	5
1	**Раздел 1.** Математические основы криптологии.	Свойства бинарных операций. Группы, полугруппы, подгруппы Теорема Лагранжа. Кольцо, поле. Системы вычетов. НОД, функция Эйлера, основная теорема арифметики. Мультипликативная инверсия, расширенный алгоритм Евклида. Малая теорема Ферма, формула Эйлера, примитивный элемент поля. Диофантовы уравнения. Решение простейших диофантовых уравнений 1 степени. Решение сравнений первой степени. Китайская теорема об остатках, решение системы сравнений. Решение квадратичных сравнений Определение простых чисел. Алгоритмы проверки на простоту. Детерминированные алгоритмы . Алгоритмы проверки на простоту. Вероятностные алгоритмы. Тест Миллера-Рабина. Общий подход к проверке числа на простоту. Задача факторизации числа, метод Ферма, методы Полларда. Точки эллиптических кривых. Операции, группа точек. Кольцо многочленов над заданным полем.	ЛР	

		Неприводимые многочлены. Примитивные многочлены. Понятие составного поля Галуа. Циклотомические классы элементов поля Галуа, с примером. Корни неприводимых многочленов из расширения поля. Циклотомические классы и минимальные многочлены в составном поле Галуа.		
2	**Раздел 2.** Криптоалгоритмы.	Математическая модель криптосистемы. Основные составляющие и термины. Типы атак на криптосистемы. Понятие стойкости шифра по Шеннону. Совершенные шифры. Классификация шифров. Криптоалгоритмы и криптопротоколы. Классические шифры. Представление данных и операции над ними в современных криптосистемах. Понятие случайной последовательности, ПСП, криптографически-стойкой ПСП, примеры. Линейный конгруэнтный метод. Метод Фиббоначи с запаздываниями. Алгоритм Блюм-Блюм-Шуба. Регистр сдвига. М-последовательность, нелинейный усложнитель. Вихрь Мерсена. Тесты NIST. Тесты DIE HARD. Общие подходы к построению блочных симметричных шифров. Обратимые и необратимые операции, классификация блочных шифров. Шифры Фейстеля. Шифр DES. Параметры и общая структура. Функция шифрования. Расширение ключей. Уязвимости. TRIPLE DES. Шифр AES. Параметры и общая структура. Структура раунда. SubBytes, AddRoundKey. Расширение ключей. ShifRows, MixColumns. Шифр Магма. Параметры и общая структура. Функция шифрования. Расширение ключей. Шифр Кузнечик. Параметры и общая структура. Структура раунда. Расширение ключей. Потоковые шифры, общий подход, примеры. RC4. RC5. A5/1. Понятие односторонней функции. Понятие криптографически односторонней функции. Первичная модель ассиметричной криптосистемы. Рюкзачная криптосистема. Недостатки рюкзачной системы, модифицированная модель ассиметричной криптосистемы. RSA. EL-gamal. Криптография в эллиптических кривых	ЛР	
3	**Раздел 3.** Криптопротоколы	Понятие хэш-функции. Понятие коллизий. Понятие криптографически стойкой хэш функции, классификация Хэшей. MD5. Sha-2. Стрибог. Построение хэшфункций на симметричных алгоритмах. Протоколы построения. Whirpool. ЭЦП. Терминология. Общие принципы и протоколы применения. DSS. ECDSA. ГОСТ 34.10-2018. Режимы работы блочных шифров. Режимы ECB и CBC. Режимы CFB и OFB. Режимы CTR и имитовставки. Режимы работы ГОСТ 34.12. Протоколы распределения ключей, протоколы с выделенным центром, общий подход и пример. Протокол Отвея-Ривса. Протокол Ниидома-Шредера. Протокол Цербер. Протокол Диффи-Хэллмана. Атака посередине. Протокол от станции к станции. X.509 PKI Модели доверия сертификационных центров.	ЛР	

2.3.2. Занятия семинарского типа

Занятия семинарского типа – не предусмотрены.

2.3.3. Лабораторные занятия

№ работы	№ раздела дисциплины	**Наименование лабораторных работ**	Форма текущего контроля
1	1	**Тема "** Элементы теории чисел**".**	Отчет по лабораторной работе
2	1	**Тема «**Решение сравнений».	-//-
3	1	**Тема** «Кольцо многочленов».	-//-
4	1	**Тема** «Поля Галуа».	-//-
5	1	**Тема** «NP-полные задачи теории чисел».	-//-
6	1	**Тема «**Группы точек эллиптических кривых»	-//-
7	1	**Тема** " Математические основы криптологии»	КР
8	2	**Тема** " ПСП»	Отчет по лабораторной работе
9	2	**Тема** " Симметричные шифры»	-//-
10	2	**Тема** " Ассиметричные шифры»	-//-
11	3	**Тема** " Применение шифров»	-//-
12	3	**Тема** " ХЭШ/ЭЦП»	-//-
13	3	**Тема** " Распределение ключей»	-//-
14	3	**Тема** " Криптоалгоритмы и криптопротоколы»	КР

Лабораторная работа № 1.

Блок 1. Введение в теорию чисел.

№ 1. Для данных пар чисел найти НОД

(256,384) (714,218) (516, 438) (735, 525)\

№ 2. Для данных чисел найти значение функции Эйлера

63, 100, 525, 31, 274

№ 3. Для заданных значений модуля найти все первообразные корни в данном поле

7, 11, 13, 19, 23

Блок 2. Диофантовы уравнения и сравнения первой степени.

№ 4. Решить заданные Диофантовы уравнения

5x+7y=14 10x+12y=1314x+27y=4918x+35y=36

27x+36y=3254x+48y=128 150x+75y=216 50x+44y=121

№ 5. Решить данное сравнение первой степени двумя способами.

5.1. $3x = 19 \bmod 34$ 5.2. $7x = 11 \bmod 39$ 5.3. $5x = 8 \bmod 21$

5.4. $15x = 35 \bmod 100$ 5.5. $9x = 21 \bmod 48$ 5.6. $14x = 8 \bmod 50$

5.7. $16x = 19 \bmod 34$ 5.8. $22x = 11 \bmod 38$ 5.9. $6x = 7 \bmod 22$

5.10. $4x = 3 \bmod 7$ 5.11. $11x = 5 \bmod 17$ 5.12. $2x = 5 \bmod 11$

Блок 3. Задания по вариантам

№ 1. Реализовать программный продукт решения сравнений первой степени с указанием всех промежуточных шагов вычисления (текущее значение коэффициентов в расширенном алгоритме Евклида), программный продукт так же должен реализовывать возможность того, что сравнение не имеет решений или имеет больше одного решения. В первом случае сообщать пользователю с пояснением, во втором строить все возможные решения.

№2. Реализовать программный продукт нахождения функции эйлера от числа двумя способами(по определению и с помощью формулы). Сравнить эффективность алгоритмов для набора из 100 чисел, каждое из которых больше 10’000’000.

№ 3. Реализовать программный продукт решения сравнений первой степени двумя способами с указанием всех промежуточных шагов вычисления (текущее значение коэффициентов расширенном алгоритме Евклида и текущее значение степеней в формуле Эйлера), программный продукт так же должен реализовывать возможность того, что сравнение не имеет решений или имеет больше одного решения. В первом случае сообщать пользователю с пояснением, во втором строить все возможные решения.

№4. Реализовать программный продукт нахождения всех первообразных корней по заданному простому модулю с указанием всех этапов нахождения корня.

№5. Реализовать программный продукт решения диофантового уравнения первой степени с помощью расширенного алгоритма Евклида с указанием всех промежуточных результатов.

Лабораторная работа № 2.

Блок 1. Китайская теорема об остатках

№ 1. Найти решение системы сравнений

$$x=2(\mathrm{mod}\ 5),$$
$$x=15(\mathrm{mod}\ 17),$$
$$x=5(\mathrm{mod}\ 12).$$

№ 2. Найти решение системы сравнений

$x=8(\mathrm{mod}\ 6)$,
$x=13(\mathrm{mod}\ 35)$,
$x=4(\mathrm{mod}\ 11)$.

Блок 2. Разные задачи

Форроузан, лекция 2, задачи № 13 – 16, 30 – 37

Форроузан, лекция 4, задачи № 8, 9, 10

Форроузан, лекция 9, задачи № 9 – 11, 19 – 22, 24

Блок 3. Задания по вариантам

№ 1. Реализовать программный продукт решения квадратичного сравнения с указанием промежуточных результатов. Программа должна показывать случаи, когда решения существуют, находить количество решений или указывать, что нахождение затруднительно.

№ 2. Реализовать программный продукт решения системы сравнений с помощью китайской теоремы об остатках с указанием промежуточных результатов (значения M, сравнения и решения сравнений первой степеней My=a mod m). Программный продукт так же должен реализовывать возможность того, что система не имеет решений или имеет больше одного решения.

№ 3. Реализовать программный продукт нахождения множества квадратичных вычетов и множества квадратичных невычетов по заданному простому модулю с пояснением всех промежуточных шагов решения задачи.

№ 4. Реализовать класс вычисления целых степеней по заданному модулю(для вычисления положительной степени воспользоватеься малой теоремой Ферма и реализованными отдельном методами умножения и сложения по заданному модулю, для вычисления отрицательной степени воспользоваться теоремой Эйлера).

Лабораторная работа № 3. Кольцо многочленов

Блок 1. Многочлены

Задание 1. Умножить и разделить многочлен на многочлен с остатком над полем $GF(2)$.

1.1. $F(x)=x^3+x+1, \quad G(x)=x+1$

1.2. $F(x)=x^2+1, \quad G(x)=x+1$

1.3. $F(x)=x^3+x^2+1, \quad G(x)=x^2+1$

1.4. $F(x)=x^4+x^2+1, \quad G(x)=x^2+x+1$

1.5. $F(x)=x^4+x^2+x+1, G(x)=x+1$

1.6. $F(x)=x^5+x^3+x^2+1, \quad G(x)=x^2+x+1$

Задание 2. Найти НОД указанных многочленов над полем $GF(2)$.

2.1. $F_1(x)=1+x^5, \ F_2(x)=1+x+x^2+x^3$

2.2. $F_1(x)=x^5+x^4+1, \quad F_2(x)=x^4+x^3+x+1$

2.3. $F_1(x)=x^4+1, \ F_2(x)=x^5+x^3+x^2+1$

2.4. $F_1(x)=x^5+x^4+x^3+x, \quad F_2(x)=x^5+x^3+x^2+x$

Задание 3. Выяснить, является ли данный многочлен неприводимым, примитивным над полем $GF(2)$.

3.1. $F(x)=x^2+1$

3.2. $F(x)=x^2+x+1$

3.3. $F(x)=x^3+1$

3.4. $F(x)=x^3+x$

3.5. $F(x)=x^3+x+1$

3.6. $F(x)=x^3+x^2$

3.7. $F(x)=x^3+x^2+1$

3.8. $F(x)=x^3+x^2+x$

3.9. $F(x)=x^3+x^2+x+1$

3.10. $F(x)=x^4+1$

3.11. $F(x)=x^4+x+1$

3.12. $F(x)=x^4+x^2$

3.13. $F(x)=x^4+x^2+1$

3.14. $F(x)=x^3+x^2+x+1$

3.15. $F(x)=x^4+x^3+1$

3.16. $F(x)=x^4+x^3+x^2+1$

3.17. $F(x)=x^4+x^3+x^2+x+1$

3.18. $F(x)=x^5+x^3+x+1$

3.19. $F(x)=x^5+x^3+x^2+1$

3.20. $F(x)=x^5+x^4+x^3+1$

3.21. $F(x)=x^5+x^4+x^3+x^2+1$

3.22. $F(x)=x^5+x^4+x^3+x+1$

3.23. $F(x)=x^5+x^4+x^2+1$

3.24. $F(x)=x^5+x^3+1$

3.25. $F(x)=x^5+x^2+1$

3.26. $F(x)=x^5+x+1$

Блок 2. Поля Галуа.

№ 4. Построить таблицу умножения в поле Галуа GF(8) с образующим многочленом 1101

№ 5. Построить таблицу умножения в поле Галуа GF(8) с образующим многочленом 1011

Блок 3. Примитивные элементы поля Галуа

№ 6. Найти примитивные элементы поля из задачи 4.
№ 7. Найти примитивные элементы поля из задачи 5
№ 8. Найти примитивные элементы поля GF(16) для образующего многочлена 11001
№ 9. Найти примитивные элементы поля GF(16) для образующего многочлена 10011
№ 10. Найти примитивные элементы поля GF(64) для образующего многочлена 1000011
№ 11. Найти примитивные элементы поля GF(64) для образующего многочлена 1001001
№ 12. Найти примитивные элементы поля GF(64) для образующего многочлена 1010111

Блок 4. Разные задачи

Форроузан, лекция 4, задачи 21 – 25

Блок 5. Задания по вариантам

№ 1. Реализовать интерактивный калькулятор в поле Галуа с заданным пользователем образующим многочленом (сложение, умножение, деление, НОД, возведение в степень и таблица умножения).

№ 2. Реализовать проверку многочлена на неприводимость и примитивность.

№ 3. Реализовать программный продукт построения всех примитивов заданного поля $GF(2^n)$. Указать все промежуточные результаты, то есть
- первичный перебор с указанием проверенных элементов поля и поянением, почему они не примитивы;
- вывод всех примитивов с указанием степеней образующего элемента.

Лабораторная работа № 4. Поля Галуа

№ 1. Выделить циклотомические классы и найти соответствующие им минимальные многочлены для поля GF(16) для образующего многочлена 11001.
№ 2. Выделить циклотомические классы и найти соответствующие им минимальные многочлены для поля GF(16) для образующего многочлена 10011.
№ 3. Для многочлена x над полем $GF(2^5)$ с образующим многочленом $x^5 + x^2 + 1$ найти циклотомический класс и минимальный многочлен.
№ 4. Для многочлена x^3 над полем $GF(2^5)$ с образующим многочленом $x^5 + x^2 + 1$ найти циклотомический класс и минимальный многочлен.
№ 5. Для многочлена x^5 над полем $GF(2^5)$ с образующим многочленом $x^5 + x^2 + 1$ найти циклотомический класс и минимальный многочлен.
№ 6. Для многочлена x^7 над полем $GF(2^5)$ с образующим многочленом $x^5 + x^2 + 1$ найти циклотомический класс и минимальный многочлен.
№ 7. Построить циклотомические классы и минимальные многочлены в поле Галуа $x^5 + x^3 + 1$

№ 8. Построить циклотомические классы и минимальные многочлены в поле Галуа $x^5+x^3+x^2+x+1$
№ 9. Проверить на примитивность неприводимый многочлен 100101
№ 10. Проверить на примитивность неприводимый многочлен 110111
№ 11. Проверить на примитивность неприводимый многочлен 1011011
№ 12. Проверить на примитивность неприводимый многочлен 1100001

Лабораторная работа № 5. NP-полные задачи теории чисел

Блок 1. Простые числа

№ 1. Привести пример пяти простых чисел Мерсена
№ 2. Привести пример четырех простых чисел Ферма.
№ 3. Провести тест Ферма для чисел 23, 41, 15, 35, 561. Каково название последнего числа?
№ 4. Провести испытание квадратным корнем для чисел 23, 41, 15, 35, 561.
№ 5. Провести тест Миллера-Рабина для чисел 23, 41, 15, 35, 561

Блок 2. Разложение на множители

№ 6. Применить метод Ферма разложения на множители для чисел 483, 1207, 561, 1219.
№ 7. Применить (p-1) метод Полларда разложения на множители для чисел 483, 1207, 561, 1219
№ 8. Применить PO(Rho) метод Полларда разложения на множители для чисел 483, 1207, 561, 1219
№ 9. Применить квадратичное решето разложения на множители для чисел 483, 1207, 561, 1219
№ 10. Применить решето поля чисел разложения на множители для чисел 483, 1207, 561, 1219

Блок 3. Разные задачи

Фороузан, лекция 9, задачи 12 – 18, 25 – 27

Блок 4. Индивидуальные задания

№ 1. Реализовать программный продукт, позволяющий проводить тест Ферма чисел на простоту. Провести от одного до ста тестов для каждого числа. Сформировать список составных чисел до одного миллиарда для которых первое прохождение теста выдает ответ простое, отметить для каждого из этих чисел, какой ответ будет выдавать тест в случае проведения от 2 до 100 тестов. Сформировать итоговую таблицу вида

число	1 тест	2	3	4	5	6	…	100
561	-	-	-	-	-	-		+

№ 2. Реализовать программный продукт, позволяющий проводить испытание квадратным корнем чисел на простоту. Провести от одного до ста тестов для каждого числа. Сформировать список составных чисел до одного миллиарда для которых первое прохождение теста выдает ответ простое, отметить для каждого из этих чисел, какой ответ будет выдавать тест в случае проведения от 2 до 100 тестов. Сформировать итоговую таблицу вида

число	1 тест	2	3	4	5	6	…	100
561	-	-	-	-	-	-		+

№ 3. Реализовать программный продукт, позволяющий проводить тест Миллера-Рабина чисел на простоту. Провести от одного до ста тестов для каждого числа. Сформировать список составных чисел до одного миллиарда для которых первое прохождение теста выдает ответ простое, отметить для каждого из этих чисел, какой ответ будет выдавать тест в случае проведения от 2 до 100 тестов. Сформировать итоговую таблицу вида

число	1 тест	2	3	4	5	6	…	100
561	-	-	-	-	-	-		+

№ 4. Реализовать алгоритм AKS проверки чисел на простоту. Вывести все простые числа до 1000000 в файл. Убедится в корректности работы алгоритма, применить стандартный алгоритм проверки на простоту.

№ 5. Реализовать приложение, позволяющее для заданного модуля находить все квадратичные вычеты и невычеты по этому модулю.

№ 6. Реализовать алгоритм быстрого возведения в степень Показать его эффективность.

№ 7. Реализовать решение квадратичного сравнения по простому модулю.

№ 8. Реализовать решение квадратичного сравнения по составному модулю.

№ 9. Реализовать (p-1) метод Полларда разложения на множители и PO(Rho) метод Полларда разложения на множители. Показать результаты для различных чисел

№ 10. Реализовать квадратичное решето разложения на множители чисел.

№ 11. Реализовать решето поля чисел разложения на множители

№ 12. Реализовать решение показательного сравнения на основе дискретного логарифма

Лабораторная работа № 6. Эллиптические кривые

Учебник Форроузан Криптография и сетевая безопасность, лекция 10,

страницы 351-358 изучить материал, выполнить упражнения 16 и 17.

Лабораторная работа № 8.

Блок 1. Линейный конгруэнтный метод.

Задание 8.1. Построить линейную конгруэнтную последовательность, удовлетворяющую заданному рекуррентному соотношению.

Вар №	№	Задача
0	8.1.1	Построить псевдослучайную последовательность чисел заданную выражением вида $X_{n+1}=(aX_n+c)$ mod m при X_0=4, a=6, c=7, m=10
	8.1.2	Построить псевдослучайную последовательность чисел заданную выражением вида $X_{n+1}=(aX_n+c)$ mod m при X_0=4, a=4, c=5, m=9
1	8.1.1	Построить линейную конгруэнтную ПСП для параметров X_0=7, a=c=7, m=10
	8.1.2	Построить псевдослучайную последовательность чисел заданную выражением вида $X_{n+1}=(aX_n+c)$ mod m при X_0=5, a=5, c=3, m=8

Задание 8.2. Приведите примеры рекуррентных соотношений, задающих линейную конгруэнтную ПСП чисел, удовлетворяющую заданным свойствам.

Вар №	№	Задача
0	8.2.1	Привести три примера задания параметров для получения случайной последовательности чисел m, a, c, X_0, имеющей период длиной 8
	8.2.2	Выяснить, существуют ли параметры a,c, задающие линейную конгруэнтную последовательность на основе РС вида $X_{n+1}=(aX_n+c)$ mod 24, имеющую период Т=24
1	8.2.1	Привести три примера задания параметров для получения случайной последовательности чисел m, a, c, X_0, имеющей период длиной 16.
	8.2.2	Выяснить, существуют ли параметры a,c, задающие линейную конгруэнтную последовательность на основе РС вида $X_{n+1}=(aX_n+c)$ mod 10, имеющую период Т=10.

Блок2. Псевдослучайные последовательности

Источник. Б.Форроузан. «Киптография и безопасность сетей» Приложение К.

8.3.1. Реализовать пример генератора последовательности Фиббоначи с запаздываниями для целых чисел.

8.3.2. Реализовать пример генератора последовательности Фиббоначи с запаздываниями для элементов произвольного поля Галуа GF(2^n)

8.4. Реализовать пример генератора Блюм-Блюм-Шуба для произвольных

параметров. Найти период, оценить период, сделать выводы.

Блок 4. Регистр сдвига.

Задание 8.5. Построить двоичную ПСП чисел, соответствующую заданному порождающему многочлену *F(x)* линейного рекуррентного регистра сдвига с заданным начальным заполнением $x_p, x_{p+1}, x_{p+2}, x_{p+3}, \dots$. Найти период полученной последовательности.

Вар №	№	Задача
0	8.5.1	$F(x)=x^4+x+1, \quad x_p=1, x_{p+1}=0, x_{p+2}=1, x_{p+3}=0$
	8.5.2	$F(x)=x^5+x^3+x, \quad x_p=1, x_{p+1}=0, x_{p+2}=1, x_{p+3}=0, x_{p+4}=1$
1	8.5.1	$F(x)=x^4+x^3+1, \quad x_p=1, x_{p+1}=0, x_{p+2}=1, x_{p+3}=0$
	8.5.2	$F(x)=x^5+x^2+1, \quad x_p=1, x_{p+1}=0, x_{p+2}=1, x_{p+3}=0, x_{p+4}=0$
2	8.5.1	$F(x)=x^4+x^3+1, \quad x_p=0, x_{p+1}=1, x_{p+2}=0, x_{p+3}=1$
	8.5.2	$F(x)=x^5+x^3+x^2+x+1, \quad x_p=0, x_{p+1}=1, x_{p+2}=1, x_{p+3}=0, x_{p+4}=1$

Задание 8.7. Дан многочлен, выяснить, является ли он неприводимым, примитивным.

Вар №	Задача
0	$F(x)=x^7+x^4+1$
1	$F(x)=x^7+x^3+1$
2	$F(x)=x^7+x^6+1$

Задание 8.8. Среди указанных двоичных последовательностей выбрать М-последовательность (максимальной длины).

8.8.1		
Из представленных псевдослучайных двоичных последовательностей М-последовательностью (максимальной длины) в соответствии со свойствами последовательности является:		
1	…11100001010110011100001010 11…	
2	…10101101010110101011010110…	
3	…00000111010111000000111010 11…	
4	…01001000011111001001000011 11…	
5	…00110101111000100110101111 00…	

8.8.2.		
Из представленных псевдослучайных двоичных последовательностей М-последовательностью (максимальной длины) в соответствии со свойствами последовательности является:		
1	…00000111010111000000111010 11…	

2	…0100100001111100100100001111…	
3	…1110000101011001110000101011…	
4	…0011101001110100111010011101…	
5	…0011010111100010011010111100…	

8.8.3.		
Из представленных псевдослучайных двоичных последовательностей М-последовательностью максимальной длины является:		
Ответы (одиночный выбор)		
1	…0000011101011100000011101011…	
2	…0100100001111100100100001111…	
3	…0011010111100010011010111100…	
4	…1010110101011010101101010110…	
5	…1110000101011001110000101011…	

8.8.4.		
Из представленных псевдослучайных двоичных последовательностей М-последовательностью максимальной длины является:		
Ответы (одиночный выбор)		
1	…1110000101011001110000101011…	
2	…1010110101011010101101010110…	
3	…0000011101011100000011101011…	
4	…0100100001111100100100001111…	
5	…0011010111100010011010111100…	

8.8.5.		
Из представленных псевдослучайных двоичных последовательностей М-последовательностью максимальной длины является:		
Ответы (одиночный выбор)		
1	…0000011101011100000011101011…	
2	…0100100001111100100100001111…	
3	…1110000101011001110000101011…	
4	…0011101001110100111010011101…	
5	…0011010111100010011010111100…	

Блок 4*.

Построить ПСП с помощью генератора ПСП вихрь Мерсена с произвольными параметрами (задача может быть выполнена вручную или построена реализация алгоритма).

Блок 5. ЗАДАЧИ ПО ВАРИАНТАМ

№ 1. Построить реализацию регистра сдвига с примитивным многочленом 10 степени;
построить реализацию регистра сдвига с примитивным многочленом 6 степени;
построить реализацию регистра сдвига с примитивным многочленом 14 степени;
построить реализацию нелинейного усложнителя для 3 аргументов;
построить реализацию вихря Мерсена.
Итого получено 5 генераторов ПСП. Использовать их для построения ПСП длиной

100, 1000 и 10000 символов, каждый в количестве 5 различных ПСП, итого получится 15 различных ПСП.
Для указанных ПСП реализовать тесты NIST № 1, 6, 12. Для каждого из тестов оценить время прохождения и итоговый результат. Собрать результаты в таблицу. Сделать выводы.

№ 2. Построить реализацию регистра сдвига с примитивным многочленом 10 степени;
построить реализацию регистра сдвига с примитивным многочленом 5 степени;
построить реализацию регистра сдвига с примитивным многочленом 15 степени;
построить реализацию нелинейного усложнителя для 3 аргументов;
построить реализацию вихря Мерсена.
Итого получено 5 генераторов ПСП. Использовать их для построения ПСП длиной 100, 1000 и 10000 символов, каждый в количестве 5 различных ПСП, итого получится 15 различных ПСП.
Для указанных ПСП реализовать тесты NIST № 2, 7, 11. Для каждого из тестов оценить время прохождения и итоговый результат. Собрать результаты в таблицу. Сделать выводы.

№ 3. Построить реализацию регистра сдвига с примитивным многочленом 10 степени;
построить реализацию регистра сдвига с примитивным многочленом 7 степени;
построить реализацию регистра сдвига с примитивным многочленом 13 степени;
построить реализацию нелинейного усложнителя для 3 аргументов;
построить реализацию вихря Мерсена.
Итого получено 5 генераторов ПСП. Использовать их для построения ПСП длиной 100, 1000 и 10000 символов, каждый в количестве 5 различных ПСП, итого получится 15 различных ПСП.
Для указанных ПСП реализовать тесты NIST № 3, 5, 10. Для каждого из тестов оценить время прохождения и итоговый результат. Собрать результаты в таблицу. Сделать выводы.

№ 4. Построить реализацию регистра сдвига с примитивным многочленом 10 степени;
построить реализацию регистра сдвига с примитивным многочленом 8 степени;
построить реализацию регистра сдвига с примитивным многочленом 12 степени;
построить реализацию нелинейного усложнителя для 3 аргументов;
построить реализацию вихря Мерсена.
Итого получено 5 генераторов ПСП. Использовать их для построения ПСП длиной 100, 1000 и 10000 символов, каждый в количестве 5 различных ПСП, итого получится 15 различных ПСП.
Для указанных ПСП реализовать тесты NIST № 4, 8, 9. Для каждого из тестов оценить время прохождения и итоговый результат. Собрать результаты в таблицу. Сделать выводы.

№ 5. Построить реализацию регистра сдвига с примитивным многочленом 10

степени;
построить реализацию регистра сдвига с примитивным многочленом 9 степени;
построить реализацию регистра сдвига с примитивным многочленом 11 степени;
построить реализацию нелинейного усложнителя для 3 аргументов;
построить реализацию вихря Мерсена.
Итого получено 5 генераторов ПСП. Использовать их для построения ПСП длиной 100, 1000 и 10000 символов, каждый в количестве 5 различных ПСП, итого получится 15 различных ПСП.
Для указанных ПСП реализовать тесты Дни Рождения, Пересекающиеся перестановки, Ранги матриц. Для каждого из тестов оценить время прохождения и итоговый результат. Собрать результаты в таблицу. Сделать выводы.

№ 6. Построить реализацию регистра сдвига с примитивным многочленом 10 степени;
построить реализацию регистра сдвига с примитивным многочленом 6 степени;
построить реализацию регистра сдвига с примитивным многочленом 14 степени;
построить реализацию нелинейного усложнителя для 3 аргументов;
построить реализацию вихря Мерсена.
Итого получено 5 генераторов ПСП. Использовать их для построения ПСП длиной 100, 1000 и 10000 символов, каждый в количестве 5 различных ПСП, итого получится 15 различных ПСП.
Для указанных ПСП реализовать тесты Обезьяньи тесты, Подсчет единичек, Тест на парковку. Для каждого из тестов оценить время прохождения и итоговый результат. Собрать результаты в таблицу. Сделать выводы.

№ 7. Построить реализацию регистра сдвига с примитивным многочленом 10 степени;
построить реализацию регистра сдвига с примитивным многочленом 5 степени;
построить реализацию регистра сдвига с примитивным многочленом 15 степени;
построить реализацию нелинейного усложнителя для 3 аргументов;
построить реализацию вихря Мерсена.
Итого получено 5 генераторов ПСП. Использовать их для построения ПСП длиной 100, 1000 и 10000 символов, каждый в количестве 5 различных ПСП, итого получится 15 различных ПСП.
Для указанных ПСП реализовать тесты Тест на минимальное расстояние, Тест случайных сфер, Тест сжатия. Для каждого из тестов оценить время прохождения и итоговый результат. Собрать результаты в таблицу. Сделать выводы.

№ 8. Построить реализацию регистра сдвига с примитивным многочленом 10 степени;
построить реализацию регистра сдвига с примитивным многочленом 7 степени;
построить реализацию регистра сдвига с примитивным многочленом 13 степени;
построить реализацию нелинейного усложнителя для 3 аргументов;
построить реализацию вихря Мерсена.
Итого получено 5 генераторов ПСП. Использовать их для построения ПСП длиной 100, 1000 и 10000 символов, каждый в количестве 5 различных ПСП, итого

получится 15 различных ПСП.
Для указанных ПСП реализовать тесты тест пересекающихся сумм, Тест последовательностей, Тест игры в кости. Для каждого из тестов оценить время прохождения и итоговый результат. Собрать результаты в таблицу. Сделать выводы.

Лабораторная работа № 9.

Задание 1. Провести 5 раунд алгоритма DES, если текущее заполнение 123456789ABCDEF, начальный ключ 3456789ABCDEF.

Задание 2. Форроузан лекция 6, задания после лекции 1 – 6.

Задание 3. На основе стандарта необходимо провести один раунд преобразования в режиме простой замены.

ГОСТ 28147-89

СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ. АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

http://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=131282

Задание 4. Провести 5 раунд алгоритма AES, для ключа 128 бит из 10 раундов, если текущее заполнение
123456789ABCDEF123456789ABCDEF,
начальный ключ 123456789ABCDEF123456789ABCDEF.

Задание 5. Форроузан лекция 7, задания после лекции 8, 13, 14.

Задание 6. На основе стандарта необходимо провести один раунд преобразования в режиме простой замены.

ГОСТ 28147-18

СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ. АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

БЛОК 2. ЗАДАНИЯ ПО ВАРИАНТАМ.

№ 1. Реализовать программный продукт прямого преобразования DES для

введенных двоичных последовательностей открытого текста и ключа. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков.

№ 2. Реализовать программный продукт прямого преобразования AES для введенных двоичных последовательностей открытого текста и ключа. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков.

№ 3. Реализовать программный продукт обратного преобразования DES для введенных двоичных последовательностей шифртекста и ключа. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков.

№ 4. Реализовать программный продукт прямого преобразования AES для введенных двоичных последовательностей шифртекста и ключа. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков.

№ 5. Реализовать программный продукт, позволяющий шифровать и расшифровывать сообщения на русском и английском языках с помощью двух блочных симметричных шифров(DES, MAGMA). Чтение открытого текста и шифртекста должно быть возможно с клавиатуры и из файла, запись результата шифрования/расшифрования возможна на экран и в файл. Ключ формируется автоматически и сохраняется на весь сеанс шифрования. Ключ сохраняется в отдельный файл. Возможно хранение нескольких ключей от разных сеансов шифрования. У пользователя есть возможность выбора, какой криптосистемой пользоваться. Шифрование реализовать для двух различных кодировок текста. Для реализации криптоалгоритмов пользоваться встроенными библиотеками используемых языков.

№ 6. Реализовать программный продукт, позволяющий шифровать и расшифровывать сообщения на русском и английском языках с помощью двух блочных симметричных шифров(TripleDES, AES). Чтение открытого текста и шифртекста должно быть возможно с клавиатуры и из файла, запись результата шифрования/расшифрования возможна на экран и в файл. Ключ формируется автоматически и сохраняется на весь сеанс шифрования. Ключ сохраняется в отдельный файл. Возможно хранение нескольких ключей от разных сеансов шифрования. У пользователя есть возможность выбора, какой криптосистемой пользоваться. Шифрование реализовать для двух различных кодировок текста. Для реализации криптоалгоритмов пользоваться встроенными библиотеками используемых языков.

№ 7. Реализовать программный продукт прямого преобразования Магма для введенных двоичных последовательностей открытого текста и ключа. Для реализации криптоалгоритмов запрещено пользоваться встроенными

библиотеками используемых языков.

№ 8. Реализовать программный продукт обратного преобразования Магма для введенных двоичных последовательностей закрытого текста и ключа. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков.

№ 9. Реализовать программный продукт, позволяющий шифровать и расшифровывать сообщения на русском языке с помощью RC5 для трех различных вариантов. Чтение открытого текста и шифртекста должно быть возможно с клавиатуры, запись результата шифрования/расшифрования на экран. Ключ формируется автоматически и сохраняется на весь сеанс шифрования. Ключ сохраняется в отдельный файл. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков.

№ 10. Реализовать программный продукт, позволяющий шифровать и расшифровывать сообщения на русском языке с помощью RC6. Чтение открытого текста и шифртекста должно быть возможно с клавиатуры, запись результата шифрования/расшифрования на экран. Ключ формируется автоматически и сохраняется на весь сеанс шифрования. Ключ сохраняется в отдельный файл. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков

№ 11. Реализовать программный продукт прямого преобразования Кузнечик для введенных двоичных последовательностей открытого текста и ключа. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков.

№ 12. Реализовать программный продукт обратного преобразования Кузнечик для введенных двоичных последовательностей открытого текста и ключа. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков.

№ 13. Реализовать программный продукт, позволяющий шифровать и расшифровывать сообщения на русском и английском языках с помощью двух блочных симметричных шифров(DES, MAGMA). Чтение открытого текста и шифртекста должно быть возможно с клавиатуры и из файла, запись результата шифрования/расшифрования возможна на экран и в файл. Ключ формируется автоматически и сохраняется на весь сеанс шифрования. Ключ сохраняется в отдельный файл. Возможно хранение нескольких ключей от разных сеансов шифрования. У пользователя есть возможность выбора, какой криптосистемой пользоваться. Шифрование реализовать для двух различных кодировок текста. Для реализации криптоалгоритмов пользоваться встроенными библиотеками используемых языков.

№ 14. Реализовать программный продукт, позволяющий шифровать и

расшифровывать сообщения на русском и английском языках с помощью двух блочных симметричных шифров(TripleDES, AES). Чтение открытого текста и шифртекста должно быть возможно с клавиатуры и из файла, запись результата шифрования/расшифрования возможна на экран и в файл. Ключ формируется автоматически и сохраняется на весь сеанс шифрования. Ключ сохраняется в отдельный файл. Возможно хранение нескольких ключей от разных сеансов шифрования. У пользователя есть возможность выбора, какой криптосистемой пользоваться. Шифрование реализовать для двух различных кодировок текста. Для реализации криптоалгоритмов пользоваться встроенными библиотеками используемых языков.

№ 15. Реализовать программный продукт прямого преобразования Магма для введенных двоичных последовательностей открытого текста и ключа. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков.

№ 16. Реализовать программный продукт обратного преобразования Магма для введенных двоичных последовательностей закрытого текста и ключа. Для реализации криптоалгоритмов запрещено пользоваться встроенными библиотеками используемых языков.

Лабораторная работа № 10

1. Дан сверхрастущий рюкзачный вектор A=(3, 5, 11, 21, 43, 87, 172, 350, 701, 1500). Построить криптосистему для данного вектора. Зашифровать фразу Iron Man. Показать процесс расшифровки.
2. Дан сверхрастущий рюкзачный вектор A=(2, 3, 6, 13, 27, 55, 112, 225, 451, 905). Построить криптосистему для данного вектора. Зашифровать фразу What’s going on? Показать процесс расшифровки.
3. Построить RSA шифр для n=35. Зашифровать фразу Iron Man. Показать процесс расшифровки.
4. Построить RSA шифр для произвольно выбранных простых чисел. Зашифровать фразу What’s going on? Показать процесс расшифровки.
5. Построить шифр El-gamal для p=31. Зашифровать фразу Iron Man. Показать процесс расшифровки.
6. Построить El-gamal шифр для произвольно выбранных простых чисел. Зашифровать фразу What’s going on? Показать процесс расшифровки.
7. Построить криптосистему Рабина для n=35. Зашифровать фразу Iron Man. Показать процесс расшифровки.
8. Построить криптосистему Рабина для произвольно выбранных простых чисел. Зашифровать фразу What’s going on? Показать процесс расшифровки.

Литература

1. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие / Фороузан Б.А.; 2010

2. Герман О.Н. Теоретико- числовые методы в криптографии / О.Н. Герман, Ю.В. Нестеренко
3. Арто Саломаа Криптография с открытым ключом

Индивидуальные задания

№ 1. Реализовать рюкзачную криптосистему шифрования и расшифрования вводимых сообщений. Открытый ключ показывать пользователю, закрытый ключ записывать в файл.

№ 2. Реализовать криптосистему RSA для шифрования и расшифрования вводимых сообщений. Открытый ключ показывать пользователю, закрытый ключ записывать в файл.

№ 3. Реализовать криптосистему El-gamal для шифрования и расшифрования вводимых сообщений. Открытый ключ показывать пользователю, закрытый ключ записывать в файл.

№ 4. Реализовать криптосистему Рабина для шифрования и расшифрования вводимых сообщений. Открытый ключ показывать пользователю, закрытый ключ записывать в файл.

№ 5. Реализовать программный продукт, позволяющий шифровать и расшифровывать сообщения на русском и английском языках с помощью двух асимметричных шифров(RSA, El-gamal). Чтение открытого текста и шифртекста должно быть возможно с клавиатуры и из файла, запись результата шифрования/расшифрования возможна на экран и в файл. Ключи формируются автоматически и сохраняются на весь сеанс шифрования. Ключи сохраняются в отдельный файл. Возможно хранение нескольких ключей от разных сеансов шифрования. У пользователя есть возможность выбора, какой криптосистемой пользоваться. Шифрование реализовать для двух различных кодировок текста. Для реализации криптоалгоритмов возможно пользоваться встроенными библиотеками используемых языков.

№ 6. Реализовать программный продукт, эмулирующий обмен зашифрованными сообщениями между двумя пользователями. Шифрование сообщения происходит любым блочным симметричным шифром в режиме электронной книги. Ключи для шифрования и расшифрования для симметричной системы формируются автоматически перед началом работы системы и доступны двум пользователям. Пользователь Алиса выбирает ключ и зашифровывает его номер произвольным ассиметричным алгоритмом. Открытый и закрытый ключ записываются в файл. Пользователь Боб принимает номер ключа шифрования, расшифровывает его и выбирает нужный ключ для обмена закрытой информацией. После чего Алиса получает открытый текст(клавиатура или файл), шифрует его установленным симметричным алгоритмом и отправляет Бобу. Боб должен его расшифровать. Шифрование реализовать для двух различных кодировок текста. Для реализации криптоалгоритмов возможно пользоваться встроенными библиотеками используемых языков.

Лабораторная работа № 11

1. Провести ХЭШ-преобразование произвольного набора длины 500 бит на основе алгоритма Стрибог(ГОСТ 34.11-2012) или реализовать данный алгоритм

Литература

1. ГОСТ 34.11-2012
2. http://eprint.iacr.org/2013/556.pdf Algebraic Aspects of the Russian Hash StandardGOST R 34.11-2012Oleksandr Kazymyrov, Valentyna Kazymyrova
3. https://xakep.ru/2016/07/20/hash-gost-34-11-2012/

Индивидуальное задание

№ 1. Реализовать программный продукт построения sha-256 для введенного текста.

№ 2. Реализовать программный продукт построения MD5 для введенного текста.

№ 3. Реализовать программный продукт построения Whirpool для введенного текста.

№ 4. Реализовать программный продукт построения Хэш-функции от введенного сообщения на блочных шифрах для произвольного блочного шифра согласно схемы Девиса-Мейера. Для построения Хэш алгоритма запрещено пользоваться готовыми библиотеками языков. Для применения блочного шифра можно пользоваться готовыми библиотеками.

№ 5. Реализовать программный продукт построения Хэш-функции от введенного сообщения на блочных шифрах для произвольного блочного шифра согласно схемы Матиса-Мейера-Осеаса. Для построения Хэш алгоритма запрещено пользоваться готовыми библиотеками языков. Для применения блочного шифра можно пользоваться готовыми библиотеками.

№ 6. Реализовать программный продукт построения Хэш-функции от введенного сообщения на блочных шифрах для произвольного блочного шифра согласно схемы Миагуччи-Пренеля. Для построения Хэш алгоритма запрещено пользоваться готовыми библиотеками языков. Для применения блочного шифра можно пользоваться готовыми библиотеками.

№ 7. Реализовать программный продукт построения sha-1 для введенного текста.

№ 8. Реализовать программный продукт построения sha-384 для введенного текста.

№ 9. Реализовать программный продукт построения SHA-3 для введенного текста.

№ 10. Реализовать программный продукт построения MD6 для введенного

текста.

Лабораторная работа № 12

1. Провести подпись и проверку подписи для алгоритма ГОСТ34.10-2018 или реализовать данный алгоритм

Литература

1. ГОСТ 34.10-2018

Индивидуальные задания

№ 1. Реализовать протокол подписания и проверки подписи файла для протокола DSS. Возможно пользоваться встроенными библиотеками языков.

№ 2. Реализовать протокол подписания и проверки подписи файла для протокола ECDSA. Возможно пользоваться встроенными библиотеками языков.

№ 3. Реализовать программный продукт, позволяющий подписывать и проверять подпись вводимого сообщения согласно схеме RSA. Возможно пользоваться встроенными библиотеками языков для хэш функции.

№ 4. Реализовать программный продукт, позволяющий подписывать и проверять подпись вводимого сообщения согласно схеме Шнора. Возможно пользоваться встроенными библиотеками языков для хэш функции.

Лабораторная работа № 13

1. Реализовать шифрование и расшифрование DES в режиме CBC, для реализации DES можно пользоваться методами библиотек.

Литература

1. Б.Форроузан — Криптография и безопасность сетей, Лекция 8.

Индивидуальные задания

№ 1. Реализовать шифрование и расшифрование DES в режиме CFB, для реализации DES можно пользоваться методами библиотек.

№ 2. Реализовать шифрование и расшифрование DES в режиме OFB, для реализации DES можно пользоваться методами библиотек.

№ 3. Реализовать шифрование и расшифрование DES в режиме CTR, для реализации DES можно пользоваться методами библиотек.

№ 4. Реализовать шифрование и расшифрование RC4.

№ 5. Реализовать шифрование и расшифрование A5/1.

№ 6. Реализовать шифрование и расшифрование AES в режиме CFB, для реализации AES можно пользоваться методами библиотек.

№ 7. Реализовать шифрование и расшифрование AES в режиме OFB, для реализации AES можно пользоваться методами библиотек.

№ 8. Реализовать шифрование и расшифрование AES в режиме CTR, для реализации DES можно пользоваться методами библиотек.

№ 9. Реализовать шифрование и расшифрование Магма в режиме гаммирования, для реализации Магма можно пользоваться методами библиотек.

№ 10. Реализовать шифрование и расшифрование Магма в режиме гаммирование с обратной связью, для реализации Магма можно пользоваться методами библиотек.

№ 11. Реализовать шифрование и расшифрование Магма в режиме выработки имитовставки, для реализации Магма можно пользоваться методами библиотек.

№ 12. Реализовать шифрование и расшифрование Кузнечик в режиме гаммирования, для реализации Кузнечик можно пользоваться методами библиотек.

№ 13. Реализовать шифрование и расшифрование Кузнечик в режиме гаммирование с обратной связью, для реализации Кузнечик можно пользоваться методами библиотек.

№ 14. Реализовать шифрование и расшифрование Кузнечик в режиме выработки имитовставки, для реализации Кузнечик можно пользоваться методами библиотек.

2.3.3 Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрены.

2.3.4 Расчетно-графические задания

Учебным планом не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3

1	**Раздел 1.** Математические основы криптологии.	Источники основной и дополнительной литературы
2	**Раздел 2.** Криптоалгоритмы.	Источники основной и дополнительной литературы
3	**Раздел 3.** Криптопротоколы	Источники основной и дополнительной литературы

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа, Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
7	Л	Компьютерные презентации и обсуждение	14
	ЛР	Разбор конкретных ситуаций (задач), тренинги по решению задач, компьютерные симуляции (программирование алгоритмов)	14
	КСР	Контрольная работа	4
Итого:			32

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

4.1 Фонд оценочных средств для проведения текущего контроля

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств итоговой аттестации (зачет в 8 семестре).

Оценка успеваемости осуществляется по результатам:

- защиты лабораторных работ;
- Выполнения контрольных работ.

Контрольная работа № 1

Вариант 0.

Для каждого номера приведены самые сложные варианты задач, которые могут выпасть, при этом в каждом номере может встретиться любая из указанных формулировок

1. Тема. Элементы теории чисел
Найти все примитивы поля Галуа GF(128).
Найти квадратичные вычеты и невычеты по модулю 31
Найти все подгруппы группы $<Z_{15}, +>$
Найти все примитивы поля по модулю 31

2. Тема Многочлены.
Построить все циклотомические классы и соответствующие им минимальные многочлены с образующим полиномом $x^5 + x^2 + 1$
Найти все примитивные элементы поля с образующим многочленом 1011011
Проверить многочлен на неприводимость 110011001
Проверить многочлен на примитивность 1000011

3. Тема Свойства структур вычетов по заданному модулю
Найти общее решение диофантового уравнения 1 степени
Найти все решения сравнения заданным методом
Найти все решения сравнения двумя методами
Провести тест Ферма проверки числа на простоту для следующих чисел 17, 41, 45, 15

4. Тема. Решение задач с использованием сравнений
Решить систему сравнений с помощью китайской теоремы об остатках
Решить квадратичное сравнение в случае простого модуля 4n + 3
Решить квадратичное сравнение в случае составного модуля
Провести испытание квадратным корнем для чисел 23, 41, 15, 35, 561

5. Алгоритмы теории чисел
Провести тест Миллера-Рабина проверки чисел 23, 41, 15, 35, 561 на простоту
Применить метод Ферма разложения на множители для чисел 483, 1207, 561, 1219
Применить (p-1) метод Полларда разложения на множители для чисел 483, 1207, 561, 1219
Применить PO(Rho) метод Полларда разложения на множители для чисел 483, 1207, 561, 1219

6. Точки эллиптической кривой
Построить все точки кривой E(1,2) в GF(11)

Построить все подгруппы группы точек кривой E(1,2) в GF(11)
Построить все точки кривой E(x^4,1) в GF(16)
Построить все подгруппы группы точек кривой E(x^4,1) в GF(16)

Контрольная работа № 2

Вариант № 0.

2. На основании многочлена 1000011 построить двоичную псевдослучайную последовательность(построить первые 20 членов и найти период)
3. Реализовать функцию DES для набора 12345678 в первом раунде DES с ключом раунда 123456789ABC
4. Реализовать метод SubBytes шифра AES для байтов 13, 18 и 186.
5. Построить шифр El-gamal для p=31. Зашифровать фразу Iron Man. Показать процесс расшифровки.
6. Показать процесс формирования и проверки электронной подписи на основе криптографии элиптических кривых для E (1, 2) , в поле GF(11)
7. Проиллюстрировать протокол Ниидома-Шредера.

4.2 Фонд оценочных средств для проведения промежуточной аттестации

Перечень вопросов к экзамену

1. Свойства бинарных операций.
2. Группы, полугруппы, подгруппы Теорема Лагранжа.
3. Кольцо, поле.
4. Системы вычетов.
5. НОД, функция Эйлера, основная теорема арифметики.
6. Мультипликативная инверсия, расширенный алгоритм Евклида.
7. Малая теорема Ферма, формула Эйлера, примитивный элемент поля.
8. Диофантовы уравнения. Решение простейших диофантовых уравнений 1 степени.
9. Решение сравнений первой степени.
10. Китайская теорема об остатках, решение системы сравнений.
11. Решение квадратичных сравнений
12. Определение простых чисел. Алгоритмы проверки на простоту. Детерминированные алгоритмы.
13. Алгоритмы проверки на простоту. Вероятностные алгоритмы.
14. Тест Миллера-Рабина. Общий подход к проверке числа на простоту.
15. Задача факторизации числа, метод Ферма, методы Полларда.
16. Точки эллиптических кривых. Операции, группа точек.
17. Кольцо многочленов над заданным полем.
18. Неприводимые многочлены. Примитивные многочлены.
19. Понятие составного поля Галуа.

20. Циклотомические классы элементов поля Галуа, с примером.
21. Корни неприводимых многочленов из расширения поля.
22. Циклотомические классы и минимальные многочлены в составном поле Галуа.

23. Математическая модель криптосистемы. Основные составляющие и термины.
24. Типы атак на криптосистемы.
25. Понятие стойкости шифра по Шеннону. Совершенные шифры.
26. Классификация шифров.
27. Криптоалгоритмы и криптопротоколы.
28. Классические шифры.
29. Представление данных и операции над ними в современных криптосистемах.
30. Понятие случайной последовательности, ПСП, криптографически-стойкой ПСП, примеры.
31. Линейный конгруэнтный метод.
32. Метод Фиббоначи с запаздываниями.
33. Алгоритм Блюм-Блюм-Шуба.
34. Регистр сдвига.
35. М-последовательность, нелинейный усложнитель.
36. Вихрь Мерсена.
37. Тесты NIST.
38. Тесты DIE HARD.
39. Общие подходы к построению блочных симметричных шифров. Обратимые и необратимые операции, классификация блочных шифров.
40. Шифры Фейстеля.
41. Шифр DES. Параметры и общая структура.
42. Шифр DES. Функция шифрования.
43. Шифр DES. Расширение ключей.
44. Шифр DES. Уязвимости. TRIPLE DES.
45. Шифр AES. Параметры и общая структура.
46. Шифр AES. Структура раунда. SubBytes, AddRoundKey.
47. Шифр AES. Расширение ключей.
48. Шифр AES. Структура раунда. ShifRows, MixColumns.
49. Шифр Магма. Параметры и общая структура.
50. Шифр Магма. Функция шифрования.
51. Шифр Магма. Расширение ключей.
52. Шифр Кузнечик. Параметры и общая структура.
53. Шифр Кузнечик. Структура раунда.
54. Шифр Кузнечик. Расширение ключей.
55. Потоковые шифры, общий подход, примеры.
56. RC4.
57. RC5.
58. A5/1.
59. Понятие односторонней функции. Понятие криптографически односторонней функции. Первичная модель ассиметричной криптосистемы.

60. Рюкзачная криптосистема.
61. Недостатки рюкзачной системы, модифицированная модель ассиметричной криптосистемы.
62. RSA.
63. EL-gamal.
64. Криптография в эллиптических кривых.
65. Понятие хэш-функции. Понятие коллизий.
66. Понятие криптографически стойкой хэш функции, классификация Хэшей.
67. MD5.
68. Sha-2.
69. Стрибог.
70. Построение хэшфункций на симметричных алгоритмах. Протоколы построения.
71. Whirpool.
72. ЭЦП. Терминология. Общие принципы и протоколы применения.
73. DSS.
74. ECDSA.
75. ГОСТ 34.10-2018.
76. Режимы работы блочных шифров. Режимы ECB и CBC.
77. Режимы работы блочных шифров. Режимы CFB и OFB.
78. Режимы работы блочных шифров. Режимы CTR и имитовставки.
79. Режимы работы ГОСТ 34.12.
80. Протоколы распределения ключей, протоколы с выделенным центром, общий подход и пример.
81. Протокол Отвея-Ривса.
82. Протокол Ниидома-Шредера.
83. Протокол Цербер.
84. Протокол Диффи-Хэллмана. Атака посередине.
85. Протокол от станции к станции.
86. X.509
87. PKI
88. Модели доверия сертификационных центров.

В рамках дисциплины рассматриваются задачи применения криптографических протоколов. Дисциплина состоит из 3 разделов. 1 раздел математическое моделирование. 2 раздел криптоалгоритмы. 3 раздел — криптографические протоколы.

По данной дисциплине форма отчетности — экзамен.

Формат проведения экзамена — 2 теоретических вопроса, 1 практическая задача или экзаменационный проект.

В рамках проведения экзамена используются процедуры допуска к экзамену и самоэкзамена. Допуск к экзамену и самоэкзамен осуществляются на основе текущего контроля успеваемости.

Контроль успеваемости осуществляется в форме проверки решения задач студентами. Каждая задача относится к одной из приведенных тем и может быть одного из следующих типов.

Тип 1. Лабораторные работы (12 штук). Выполнить все задания из ЛР, выполнить задачи по вариантам, ответить на теоретические вопросы преподавателя при защите. Допуск — 4 ЛР. По итогам защиты работ преподаватель выставляет оценку, среднее арифметическое оценок — итоговая оценка за защиты ЛР.

Тип 2. Контрольные работы. Ключевые и наиболее сложные с точки зрения понимания общего подхода к решению задачи выделяются в контрольные работы. Каждая контрольная работа содержит 6 заданий. Допуск по 2 задания в каждой КР, удовлетворительно 4 задания, хорошо 5 заданий, отлично 6 заданий.

Тип 3. Экзаменационный проект. Представить проект по криптографии на основе одной из предложенных тем. Составить отчет и презентацию. Экзаменационный проект оценивается по 4-х балльной шкале (2 — 5). Допуск — выполненный проект(наличие программы, отчета и презентации).

Студент считается допущенным к экзамену в случае, если в каждой из КР выполнено по 2 задания, защищено 4 ЛР и выполнен экзаменационный проект.

Если студент не получил допуск в течении семестра, он пишет работу на консультации и перед началом экзамена (работа из 6 заданий, в зависимости от работы в течении семестра необходимо выполнить от 2 до 6 заданий). Если студент не может выполнить задания на допуск, считается, что студент не допущен к экзамену и получает оценку неудовлетворительно)

Итого получаем 4 оценки (допуск полагается оценкой 2, самоэкзамен выставляется как среднее арифметическое 4 оценок. Оценка удовлетворительно от 3 до 3.5, оценка хорошо от 3.75 до 4.25, оценка отлично от 4.5 до 5 соответственно.

Если студента оценка не устраивает, экзамен проходит в стандартном формате.

Критерии оценивания к экзамену:

Оценка **“отлично”** - .студент корректно раскрывает оба теоретических вопроса, решает практическую задачу, криптоалгоритмы и протоколы, их сущность, место применения и безопасность раскрыты полностью, математические модели построены верно.

Оценка **“хорошо”** - .студент корректно раскрывает оба теоретических вопроса, решает практическую задачу, при этом в одном из вопросах и задаче, или в двух вопросах возможны нестрогие ошибки, криптоалгоритмы и протоколы, их сущность, место применения и безопасность раскрыты полностью, математические модели построены верно, но возможно не полностью раскрыть все этапы алгоритма, или нестрого ошибиться в математических расчетах.

Оценка **“удовлетворительно”** - .студент корректно раскрывает оба теоретических вопроса, решает практическую задачу, при этом в вопросах и задаче возможны ошибки, криптоалгоритмы и протоколы, их сущность, место применения и безопасность раскрыты полностью, математические модели построены верно, но возможно не раскрыть все этапы алгоритма, но раскрыть структуру алгоритма или протоколы, возможно ошибиться в математических расчетах, но понимать и раскрыть, на каких математических моделях построена безопасность алгоритмов.

Оценка **«не удовлетворительно»** - один из вопросов не раскрыт полностью, или допущены строгие ошибки в структуре алгоритмов или показана ошибочная математическая модель протокола или алгоритма.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья

и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

– Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 Основная литература:

1. Информационный мир XXI века. Криптография - основа информационной безопасности / под редакцией Э. А. Болелова ; Московский государственный технический университет гражданской авиации. - 5-е изд. - Москва : Издательско-торговая корпорация "Дашков и К°", 2021. - 125 с. : ил. - (Библиотека "Книга будущего инженера"). - Библиогр.: с. 124-125. - ISBN 978-5-394-04260-7 : 83 р. - Текст : непосредственный.

2. Романьков, Виталий Анатольевич. Алгебраическая криптология : монография / В. А. Романьков ; Министерство науки и высшего образования Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего образования Омский государственный университет имени Ф. М. Достоевского. - Омск : Изд-во Омского государственного университета, 2020. - 261 с. : ил. - Библиогр.: с. 240-258. - ISBN 978-5-7779-2491-9 : 300 р. - Текст : непосредственный.

3. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г.А. Ганеш ; под ред. С. М. Молявко ; пер. с англ. В. Д. Хорева. - 4-е изд. - Москва : Лаборатория знаний, 2020. - 428 с. - URL: https://e.lanbook.com/book/151552 (дата обращения: 13.04.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-00101-700-4. - Текст : электронный.

4. Майстренко, Н. В. Основы теории информации и криптографии: учебное электронное издание : учебное пособие / Н. В. Майстренко, А. В. Майстренко. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 81 с. : табл., граф., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=570354 (дата обращения: 04.07.2022). – Библиогр. в кн. – ISBN 978-5-8265-1950-9. – Текст : электронный.

5.2 Дополнительная литература:

1. Фороузан Б.А. Ф79 Криптография и безопасность сетей: Учебное пособие / Фороузан Б.А..; пер. с англ. под ред. А.Н. Берлина. — М.: Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2010. — 784 с.: ил., табл. — (Основы информационных технологий).

2. К.Айерлэнд, М.Роузен КЛАССИЧЕСКОЕ ВВЕДЕНИЕ В СОВРЕМЕННУЮ ТЕОРИЮ ЧИСЕЛ М.:Мир, 1987,416 с

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с. — 3000 экз. — ISBN 5-89392-055-4..

4. Саломаа А. С20 Криптография с открытым ключом: Пер. с англ. — М.: Мир, 1995. — 318 с., ил. ISBN 5–03–001991–X

5. ГОСТ 34.10-2018 Информационная технология КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ Процессы формирования и проверки электронной цифровой подписи Москва Стандартинформ 2018

6. ГОСТ Р 34.11-2012 Группа П85 НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ Информационная технология КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ Функция хэширования Information technology. Cryptographic data security. Hash-function ОКС 35.040 ОКСТУ 5002 Дата введения 2013-01-01

7. http://eprint.iacr.org/2013/556.pdf Algebraic Aspects of the Russian Hash StandardGOST R 34.11-2012Oleksandr Kazymyrov, Valentyna Kazymyrova

8. https://xakep.ru/2016/07/20/hash-gost-34-11-2012/

9. Герман О.Н. Теоретико- числовые методы в криптографии / О.Н. Герман, Ю.В. Нестеренко

10. . ГОСТ 28147-89 СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ. АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ http://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=131282

11. ГОСТ 28147-18 СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ. АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/

6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных работ, контрольной работы, зачета и экзамена.

Важнейшим этапом курса является самостоятельная работа по дисциплине с использованием указанных литературных источников и методических указаний автора курса. Стоит отметить, что в рамках самостоятельной работы происходит разработка согласно Agile методологии и выполнение спринтов к четко обозначенным срокам.

Виды и формы СР, сроки выполнения, формы контроля приведены выше в данном документе.

Для лучшего освоения дисциплины при защите ЛР студент должен ответить на несколько вопросов из лекционной части курса.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

7.1 Перечень информационных технологий

Проверка домашних заданий и консультирование посредством электронной почты.
Использование электронных презентаций при проведении лекций и практических занятий.

7.2 Перечень необходимого программного обеспечения

1. OS Windows, MS Office
2. Java SDK.
3. NetBeans или Intellij Idea или Eclipse.
4. GIT-ядро
5. PHP фреймворкYii. 16
6. Apache.
7. PHP.
8. Программы для демонстрации и создания презентаций («Microsoft Power Point»)

7.3 Перечень информационных справочных систем:

1. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения

Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	PowerPoint. ауд. 129, 131, А305.
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Аудитория, (кабинет) – компьютерный класс
Учебные аудитории для проведения лабораторных работ. Лаборатория…	Мебель: учебная мебель Технические средства обучения: компьютер	Лаборатория, укомплектованная специализированными техническими средствами обучения – компьютерный класс, с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета (лаб. 102-106.).

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Помещение для самостоятельной работы обучающихся (ауд._____)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	1. OS Windows, MS Office 2. Java SDK. 3. NetBeans или Intellij Idea или Eclipse. 4. GIT-ядро 5. PHP фреймворкYii. 16 6. Apache. 7. PHP. 8. Программы для демонстрации и создания презентаций («Microsoft Power Point»)