МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра теоретической информатики

УТВЕРЖДАЮ
Декан факультета ИВТ
_____ Д.Ю. Чалый
«_24_» ___мая_____ 2022 г.

Рабочая программа дисциплины
«Математические основы защиты информации и информационной безопасности**»**

Научная специальность

1.1.5 Математическая логика, алгебра, теория чисел и дискретная математика

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 15 марта 2022 г.,
протокол № 8

Программа одобрена НМК
факультета ИВТ
протокол № 6 от
18 апреля 2022 г.

Ярославль

1. Цели освоения дисциплины

Дисциплина «Математические основы защиты информации и информационной безопасности» обеспечивает приобретение знаний и умений в соответствии с ФГОС ВПО, содействует расширению научного кругозора аспиранта, формированию представления о современном состоянии теоретической информатики и приобретению специальных знаний из области моделирования и анализа сложных информационных систем.

Цель изучения дисциплины состоит в приобретении знаний и умений в области защиты информации от несанкционированного доступа.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина «Математические основы защиты информации и информационной безопасности» является дисциплиной по выбору. Данная дисциплина направлена на подготовку к сдаче кандидатского экзамена по научной специальности 1.1.5 Математическая логика, алгебра, теория чисел и дискретная математика.

3. Планируемые результаты обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы аспирантуры, и критерии их оценивания

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Знать:

- наиболее известные симметричные криптосистемы;
- наиболее известные криптосистемы открытого ключа;
- наиболее известные системы псевдослучайных генераторов;

Уметь:

- шифровать информацию с помощью различных симметричных криптосистем;
- шифровать информацию с помощью различных криптосистем открытого ключа
- шифровать информацию с помощью различных криптосистем поточного шифрования

Владеть

- навыками построения модели информационной безопасности.
- навыками создавать ЭЦП;
- навыками работы с ключами.
- навыками вычисления хэш функций.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 акад.часов.

Дисциплина изучается в течение двух семестров. Формой итоговой промежуточной аттестации по дисциплине в последнем семестре ее изучения является зачёт.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)					Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			лекции	практические	лабораторные	консультации	самостоятельная работа	
1.	**Раздел 1.** Введение, модели безопасности, понятие компьютерной атаки. Краткий исторический обзор развития криптографии. Симметрические шифры.	2	5	3			20	Самостоятельная работа
2.	**Раздел 2.** Алгебраические структуры, используемые в криптографии. Проверка чисел на простоту. Ассиметричные криптосистемы.	2	5	3			20	Самостоятельная работа
3.	**Раздел 3.** Потоковое кодирование	2	6	4		2	18	Самостоятельная работа
	Всего за 2 семестр		16	10		2	22	Зачёт
	Всего		**16**	**10**		**2**	**80**	

Содержание разделов дисциплины:

Раздел 1. Введение, модели безопасности, понятие компьютерной атаки. Краткий исторический обзор развития криптографии. Симметрические шифры.

- Понятие конфиденциальности, целостности, доступности информации. Модели безопасности. Понятие информационной безопасности.
- История защиты информации. Исторические системы (Цезарь, Хилл, аффинная), одно алфавитные и много алфавитные системы (система Плейфейра, Виженера, Бьюфорта)
- Симметричные шифры. Возможные схемы построения симметричных шифров: схема Фейстеля, схема SP-сеть, схема квадрат. Режимы шифрования, гаммирование. Алгоритмы DES, Blowfish, Гост28147-89, AES, RC6,Serpent, Mars

Раздел 2. Алгебраические структуры, используемые в криптографии. Проверка чисел на простоту. Ассиметричные криптосистемы.

- Алгебраические структуры: группы, кольца, поля. Нахождение мультипликативного элемента.
- Проверка чисел на простоту:
  - тест Соловея-Штрассена
  - тест Миллера-Рабина
- Ассиметричные криптосистемы:
  - рюкзачная криптосистема; построение криптосистемы; теория достижимости. модификация рюкзачной криптосистемы.
  - криптосистема RSA; построение криптосистемы и криптоанализ.
  - криптосистемы Эль-Гамаля, Рабина, Вильямса, Уильемса.

Раздел 3. Потоковое кодирование

- Классификация поточных шифров (синхронные и самосинхронизирующиеся)
- Генераторы псевдослучайных последовательностей:

- Конгруэнтные генераторы и их криптоанализ.
- Регистры сдвига LFSR и их криптоанализ.
- Аддитивные генераторы
- Генераторы, построенные с использованием блоков стохастического преобразования

- Алгоритмы поточного кодирования:A5, RC4, Seal, Wake.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует аспиранта в системе изучения данной дисциплины. Аспиранты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).

В процессе осуществления образовательного процесса используются:

1 – для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система LaTex;

2 – для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next");

3 Научная электронная библиотека – http://elibrary.ru.

4 «Университетская библиотека online» – www.biblioclub.ru

– Интернет-ресурсы:

5 Системы поиска в сети Интернет – www.yandex.ru и www.google.com.

6 Правовые базы данных – Консультант+ и Гарант.

7 Сетевая модель spu2-2 http://prepod2000.kulichki.net/item_326.html

8 Имитационная модель http://graphonline.ru/

1. **7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**
2. **а) основная литература:**
3. 1. Нестеров С. А., Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров, М., Юрайт, 2016, 321с
4. 2. Гашков, С. Б., Криптографические методы защиты информации : учеб. пособие для вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев, М., Академия, 2010, 298с

3. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 2 [Электронный ресурс] : метод. указания (сост. М. В. Краснов), Ярославль, ЯрГУ, 2011, 44с

5.
6. **б) дополнительная литература:**
7. 1. Лопатин В. Н. Информационная безопасность России: Человек.Общество.Государство. / В. Н.Лопатин - СПб.: Университет, 2000. - 426с.
8. 2. Мельников В. П. Информационная безопасность и защита информации: учеб. пособие для вузов. / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова; УМО по университет. политехн. образованию - М.: Академия, 2006. - 331 с.
9. 3. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493175 (16.01.2019).
10. 4. В.И. Аверченков Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Издательство «Флинта», 2016. - 224 с. [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93351 .
11. 5. Ш.Т. Ишмухаметов Математические основы защиты информации: Электронное учебное пособие для студентов института вычислительной математики и информационных технологий / Ш.Т. Ишмухаметов, Р.Г. Рубцова. - Казань: Казанский федеральный университет, 2012. - 138 с. [Электронный ресурс]. - URL: http://window.edu.ru/resource/128/78128/files/mzi.pdf .

в) ресурсы сети «Интернет»:

1. Ш.Т. Ишмухаметов Математические основы защиты информации: Электронное учебное пособие для студентов института вычислительной математики и информационных технологий / Ш.Т. Ишмухаметов, Р.Г. Рубцова. - Казань: Казанский федеральный университет, 2012. - 138 с. [Электронный ресурс]. - URL: http://window.edu.ru/resource/128/78128/files/mzi.pdf

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

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
-учебные аудитории для проведения занятий лекционного типа и практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, хранящиеся на электронных носителях и обеспечивающие тематические иллюстрации, соответствующие рабочим программам дисциплин.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров)– списочному составу группы обучающихся.

Автор(ы) :

Профессор кафедры ТИ, д.ф.-м.н. Тимофеев Е.А.

Приложение №1 к рабочей программе дисциплины
«Математические основы защиты информации и информационной безопасности»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации аспирантов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1.Задания для самостоятельной работы

Пример заданий для самостоятельной работы к разделу 1
Формируемая компетенция:

Задания	Ответы:
1. Постройте аффинную криптосистему $f(x)=(ax+b) \bmod m$, для русского алфавита. Закодируйте число 17, предположим m=41	Числовые значения могут отличаться от тех, которые приведены в данном решении Напомним, что аффинная криптосистема определяется тремя натуральными числами Шифрование происходит заменой символа с порядковым номером на символ порядковыйномер которого вычисляется по формуле $f(x)=(ax+b) \bmod m$. Заметим, что на пару чисел и наложено условие взаимной простоты. Закодируйте слово «кокос». Будем рассматривать $f(x)=(8x+2) \bmod 41$. Нам надо закодировать В результате получим
2.Постройте криптосистему Хилла, зашифруйте «HELP», предполагая $d=2, m=26$	Числовые значения могут отличаться от тех, которые приведены в данном решении. $M=\begin{pmatrix}3&3\\2&5\end{pmatrix}\ P_1=\begin{pmatrix}H\\E\end{pmatrix}=\begin{pmatrix}7\\4\end{pmatrix}\ P_2=\begin{pmatrix}L\\P\end{pmatrix}=\begin{pmatrix}11\\15\end{pmatrix}$ Будем считать Выполним шифрование $MP_1=\begin{pmatrix}7\\8\end{pmatrix}=\begin{pmatrix}H\\I\end{pmatrix}=C_1 \quad MP_2=\begin{pmatrix}0\\19\end{pmatrix}=\begin{pmatrix}A\\T\end{pmatrix}=C_2$ Ответ «HIAT»
3.Криптосистема AES. Применим процедуру MixColunms к вектору $(a0,b4,52,ae)$, другими словами мы должны вычислить $s'(x)=s(x)\otimes g(x)$, где $s(x)=\{ae\}x^3+\{52\}x^2+\{b4\}x+\{a0\}.$ $g(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}.$	В результате получим вектор $(e0,cb,19,9e)$
4.Выполните зашифрование исходного сообщения “PURPLE” под ключевым словом “CRYPTO” с помощью системы Виженера	В результате получим “RLPEES”
5.Запрограмируйте на одном из языков программирования алгоритм RC6	Программа должна обладать следующими параметрами: • иметь графический интерфейс • выполнять процедуру шифрования и дешифрования • возможность изменять зашифрованный текст • должно быть несколько режимов

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	**Знать:** наиболее известные симметричные криптосистемы; **Уметь:** шифровать информацию с помощью различных симметричных криптосистем; **Владеть** навыками построения модели информационной безопасности.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но допустил одну вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
2	**Знать:** наиболее известные симметричные криптосистемы; **Уметь:** шифровать информацию с помощью различных симметричных криптосистем; **Владеть** навыками построения модели информационной безопасности.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но допустил одну вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
3	**Знать:** наиболее известные симметричные криптосистемы; **Уметь:** шифровать информацию с помощью различных симметричных криптосистем; **Владеть** навыками построения модели информационной безопасности.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но допустил вычислительную ошибку. 2 балла – студент полностью разобрался в решении задачи
4	**Знать:** наиболее известные симметричные криптосистемы; **Уметь:** шифровать информацию с помощью различных симметричных криптосистем; **Владеть** навыками построения модели информационной безопасности.	0 баллов – студент полностью неверно решил задачу 2 балла – студент полностью разобрался в решении задачи
5	**Знать:** наиболее известные симметричные криптосистемы; **Уметь:** шифровать информацию с помощью различных симметричных криптосистем; **Владеть**	0 баллов – студент полностью неверно решил задачу (не смог запрограммировать) 1 балл – студент верно запрограммировал алгоритм, но сделал только режим «Электронная книга» или не сделал графического интерфейса. 2 балла – студент полностью разобрался в решении задачи

	навыками построения модели информационной безопасности.	

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 5 баллов— оценка «неудовлетворительно», компетенция не сформирована;
- от 6 до 7 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 8 до 9 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
- 10 баллов— оценка «отлично», высокий уровень формирования компетенции.

Пример заданий для самостоятельной работы к разделу 2
Формируемая компетенция:

Задания	Ответы:
1.Найдите мультипликативно обратный элемент для числа 7 по модулю 101 с помощью расширенного алгоритма Евклида	В результате получим мультипликативно обратный элемент 29
2. Построить криптосистему Эль-Гамаляи закодируйте число 7	Числовые значения могут отличаться от тех, которые приведены в данном решении Криптосистема Эль-Гамаля строится следующим образом: • сначала выбирается большое простое число • выбирается число которое является примитивным для • выбирается случайное натуральноечисло причем • вычисляем Для того чтобы зашифровать сообщение надо выполнить следующие действия: • выбрать случайное натуральное число такое что числа и взаимно простые. • вычислить и Пара чисел и есть шифрованный текст Для того чтобы расшифровать сообщение, надо вычислить Построим криптосистемуЭль-Гамаля и закодируем число 7 Строим криптосистему • выбираем выбираемсекретный ключ • вычисляем Для того чтобы зашифровать сообщение надо выполнить следующие действия: • выбрать случайное натуральное число заметим, что числа 7 и 12 взаимно простые. • вычислить и Шифрованный текст – пара чисел
3.Постройте криптосистему Уильемса закодировать	Числовые значения могут отличаться от тех, которые приведены в данном решении Проектирование системы Должно выполняться для символов Лежандра

	$\varepsilon_p = \left(\frac{c}{p}\right)$ $\varepsilon_q = \left(\frac{c}{q}\right)$ $s_t \equiv -t(\bmod 4)$ для $t = p$ и $t = q$ Возьмем $c = 5$. Мы также можем выбрать $s = 2$, потому что $\left(\frac{s^2-c}{n}\right) = \left(\frac{-1}{11}\right)\left(\frac{-1}{13}\right) = -1*1 = -1$ Далее вычисляем $m = \frac{10*14}{4} = 35$. Пусть $e = 23$ $d = 16$, поскольку выполняется $ed \equiv \frac{m+1}{2}(\bmod m)$ Кодирование в нужную форму В зависимости от того, равен символ Якоби $\left(\frac{w^2-c}{n}\right)$ +1 или -1, полагаем $b_1 = 0$ и $\gamma = w + \sqrt{c}$ Или $b_1 = 1$ и $\gamma = (w + \sqrt{c})(s + \sqrt{c})$ Кодирование завершается $a = \frac{\gamma}{\bar{\gamma}}$ Шифрование Получим $b_1 = 0$, $\gamma = 21 + \sqrt{5}$ и $a = -125 + a\sqrt{5}(\bmod 143)$. Поскольку 125 нечетно, то $b_2 = 1$. Шифрование завершается нахождением $X_e(a)$ и $Y_e(a)$. Дальше вычисляем $E = (X_e(a)Y_e^{-1}(a)) \bmod n$ В результате получим ответ тройку $(E, b_1, b_2) = (28, 0, 1)$
4.Взлом рюкзачной криптосистемы дан открытый ключ $B = (4,3,2)$	Числовые значения могут отличаться от тех, которые приведены в данном решении Получим ответ $A = (1,4,7), 4, 13$

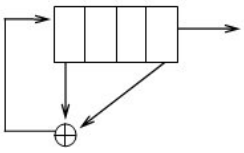
Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
2	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи

3	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
4	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	0 баллов – студент полностью неверно решил задачу 2 балла – студент полностью разобрался в решении задачи

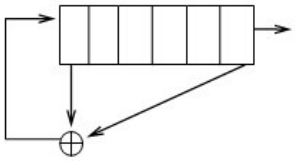
Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов— оценка «неудовлетворительно», компетенция не сформирована;
- от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 5 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов— оценка «отлично», высокий уровень формирования компетенции

Пример заданий для самостоятельной работы к разделу 3
Формируемая компетенция:

<table>
<tr><td>Задания</td><td>Ответы:</td></tr>
<tr><td>1. Постройте регистр сдвига с линейной обратной связью с ассоциированным многочленом x^4+x+1 и выпишем состояние регистра, если он был инициализирован вектором (0,0,0,1).</td><td> 
<table>
<tr><td colspan="2">Состояние регистра</td><td>выход</td><td colspan="2">Состояние регистра</td><td>выход</td></tr>
<tr><td>итерация</td><td>состояние рег. стало</td><td></td><td>итерация</td><td>состояние рег. стало</td><td></td></tr>
<tr><td>0</td><td>0001</td><td></td><td>9</td><td>1101</td><td>0</td></tr>
<tr><td>1</td><td>1000</td><td>1</td><td>10</td><td>0110</td><td>1</td></tr>
<tr><td>2</td><td>1100</td><td>0</td><td>11</td><td>0011</td><td>0</td></tr>
<tr><td>3</td><td>1110</td><td>0</td><td>12</td><td>1001</td><td>1</td></tr>
<tr><td>4</td><td>1111</td><td>0</td><td>13</td><td>0100</td><td>1</td></tr>
<tr><td>5</td><td>0111</td><td>1</td><td>14</td><td>0010</td><td>0</td></tr>
<tr><td>6</td><td>1011</td><td>1</td><td>15</td><td>0001</td><td>0</td></tr>
<tr><td>7</td><td>0101</td><td>1</td><td></td><td></td><td></td></tr>
<tr><td>8</td><td>1010</td><td>1</td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>2.Создайте комбинирующий генератор, состоящий из двух регистров сдвига с линейной обратной связью.
Первый регистр с ассоциированным многочленом</td><td>Напомним, что комбинирующий генератор проиллюстрировать следующей схемой
 

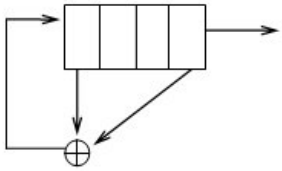
Решение
• Первый регистр</td></tr>
</table>

x^6+x+1, он был инициализирован вектором (111111). Выход регистра y_1.
Второй регистр с ассоциированным многочленом x^6+x+1 он был инициализирован вектором .
Выход регистра y_2
В качестве комбинирующей функции возьмем $f(y_1, y_2) = y_1 * y_2$
Постройте 7 битную псевдослучайную последовательность



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	y_1	итерация	состояние рег. стало	y_1
0	111111		4	101011	1
1	011111	1	5	010101	1
2	101111	1	6	101010	1
3	010111	1	7	110101	0

- Второй регистр



Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало		итерация	состояние рег. стало	
0	0001		9	1101	0
1	1000	1	10	0110	1
2	1100	0	11	0011	0
3	1110	0	12	1001	1
4	1111	0	13	0100	1
5	0111	1	14	0010	0
6	1011	1	15	0001	0
7	0101	1			
8	1010	1			

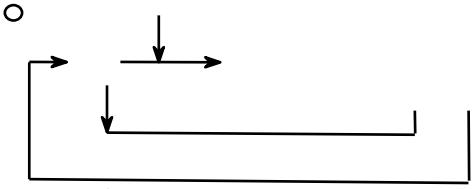
В результате получим последовательность 1000110

3. Построим стохастический генератор, ассоциированный с многочленом x^6+x^3+1 и с ключевой таблицей .
Предположим, что начальным состоянием генератора является массив .

Пусть ключевая таблица H

ключевая таблица	адрес	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
		2	1	0	12	5	3	13	10	5	14	8	7	11	9	15

Напомним, что
Результат преобразования вычисляется по формуле
где - адрес ячейки таблицы содержащей код то есть
Схема генератора

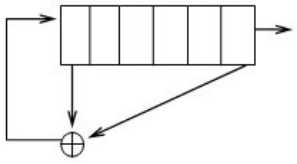
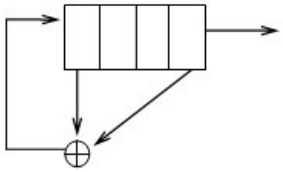


Пример работы генератора

такт	выход	заполнение регистров	такт	выход	заполнение регистров
1	9	(9,12,2,0)	5	14	(14,14,3,2)
2	2	(2,9,12,2)	6	10	(10,14,14,3)
3	3	(3,2,9,12)	7	11	(11,10,14,14)
4	14	(14,3,2,9)	8	10	(10,11,10,14)

4.Создайте

Напомним, что сжимающий генератор описывается следующим образом:

сжимающий генератор, состоящий из двух регистров сдвига с линейной обратной связью. Первый регистр с ассоциированным многочленом x^5+x+1, он был инициализирован вектором (11111). Выход регистра y_1. Второй регистр с ассоциированным многочленом x^4+x+1 он был инициализирован вектором . Выход регистра y_2	Используется 2 регистра с линейной обратной связью. Тактовые импульсы поступают на оба LFSR. Предположим, что $b=b_0b_1b_2\ldots$ последовательность с выхода LFSR1. $c=c_0c_1c_2\ldots$ - последовательность с выхода LFSR2, Тогда результирующая последовательность $z=z_0z_1z_2\ldots$ включает в себя те биты b_i для которых соответствующие биты $c_i=1$. Остальные биты последовательности b игнорируются. Решение • Первый регистр  • Второй регистр  В результате получим последовательность 1110….

Первый регистр

Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало	y_1	итерация	состояние рег. стало	y_1
0	111111		4	101011	1
1	011111	1	5	010101	1
2	101111	1	6	101010	1
3	010111	1	7	110101	0

Второй регистр

Состояние регистра		выход	Состояние регистра		выход
итерация	состояние рег. стало		итерация	состояние рег. стало	
0	0001		9	1101	0
1	1000	1	10	0110	1
2	1100	0	11	0011	0
3	1110	0	12	1001	1
4	1111	0	13	0100	1
5	0111	1	14	0010	0
6	1011	1	15	0001	0
7	0101	1			
8	1010	1			

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	**Знать:** наиболее известные системы псевдослучайных генераторов; **Уметь:** шифровать информацию с помощью различных криптосистем поточного шифрования **Владеть:** навыками вычисления хэш функций.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
2	**Знать:**	0 баллов – студент полностью неверно решил задачу

	наиболее известные системы псевдослучайных генераторов; **Уметь:** шифровать информацию с помощью различных криптосистем поточного шифрования **Владеть:** навыками вычисления хэш функций	1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
3	**Знать:** наиболее известные системы псевдослучайных генераторов; **Уметь:** шифровать информацию с помощью различных криптосистем поточного шифрования **Владеть:** навыками вычисления хэш функций	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
4	**Знать:** наиболее известные системы псевдослучайных генераторов; **Уметь:** шифровать информацию с помощью различных криптосистем поточного шифрования **Владеть:** навыками вычисления хэш функций	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов— оценка «неудовлетворительно», компетенция не сформирована;
- от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 5 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов— оценка «отлично», высокий уровень формирования компетенции

Пример заданий для самостоятельной работы к разделу 4
Формируемая компетенция:

Задания	Ответы:
1. Сформулировать алгоритм установки ЭЦП Эль-Гамаля	Числовые значения могут отличаться от тех, которые приведены в данном решении Схема ЭЦП строится следующим образом: • сначала выбирается большое простое число • выбираем число которое является примитивным элементом поля • выбираем случайное число причем • вычисляется число $y = g^x \bmod p$ Установка подписи • генерируем число $k: \{1 < k < p-1\}$ причем k и $p-1$ взаимно просты • вычисляем $a = g^k \bmod p$ и $b = [(M - xa)k^{-1}] \bmod (p-1)$ Подпись (a,b) Дан текст с хэш значением равным 5. Выполните установку ЭЦП • выбираем числа • вычисляем $y = g^x \bmod p = 2^8 \bmod 11 = 3$

	• выбираем число $k=3$ • вычисляем $a=g^k \bmod p=2^3 \bmod 11=8$ и $b=[(kr-xm)x^{-1}] \bmod (p-1)=7(5-8*3) \bmod 10=7$ Подпись (8,7)
2. Сформулировать алгоритм установки ЭЦП Гост Р34.10-94. Дан текст с хэш значением равным 3. Выполните установку ЭЦП Гост Р34.10-94	Числовые значения могут отличаться от тех, которые приведены в данном решении Схема ЭЦП строится следующим образом: • сначала выбирается большое простое число p • выбирается простое число q которое является делителем $p-1$ • выбирается натуральное число $g(1<g<p-1)$, такое что $g^q \bmod p=1$ • целое число x, меньше q • вычисляем $y=g^x \bmod p$ Установка подписи для m • генерируем число k, причем $k<q$ • вычисляем значение переменных r и s $r=(g^k \bmod p) \bmod q$ и $s=(xr+km) \bmod q$ Если $r=0$, то выбираем другое значение k и начинаем снова. Дан текст с хэш значением равным 3. Выполните установку ЭЦП • выбираем $p=11, q=5, x=3$ • выбираем $k=3$ • вычисляем $y=g^x \bmod p=4$ • выбираем $k=4$ • вычисляем $r=(g^k \bmod p) \bmod q=7$ и $s=(xr+km) \bmod q=10$ Ответ подписи (7,10)
3. Сформулировать алгоритм установки ЭЦП DSA. Дан текст с хэш значением равным 7. Выполните установку ЭЦП DSA	Числовые значения могут отличаться от тех, которые приведены в данном решении Схема DSA строится следующим образом: • сначала выбирается большое простое число p • выбирается простое число q которое является делителем $p-1$ • выбирается натуральное число g которое $g^{\frac{p-1}{q}} \bmod p=1$. Если число $g^{\frac{p-1}{q}} \bmod p=1$, то выбираем другое число g. В противном случае $g=g^{\frac{p-1}{q}} \bmod p$. • выбирается натуральноечисло x которое является секретным ключом причем $x<q$ • вычисляем $y=g^x \bmod p$ Установка подписи: • проверяем выполняется ли условие для хэш значение m текста M, что $m \bmod q \neq 0$ • выбирается натуральноечисло k, $(0<k<q)$. • вычисляем k^{-1}, для которого выполняется условие $k*k^{-1}=1 \bmod q$ • вычисляем два числа r и s по следующим правилам: $r=(g^k \bmod p) \bmod q$ $s=k^{-1}(xr+m) \bmod q$ и

	Если не выполняются условия поменяйте входные параметры. Подписью является пара чисел Проверка подписи Предположим, что к нам пришло сообщение с хэш значением и подписью • если хотя бы одно из условий не выполняется, то подпись считается недействительной • вычисляем • вычисляем: • проверяем условие Если оно выполняется то подпись считается подлинной а сообщение –неизмененным. Дан текст с хэш значением равным 7. Выполните установку ЭЦП DSA. Строим схему DSA • выбираем • вычисляем • выбираем • вычисляем Установка подписи: • выбираем • вычисляем: , , Подписью является пара чисел
(проверка)	
Задания	Ответы:
1.Запрограмируйте на одном из языков программирования алгоритм вычисления хэш функции MD5	Программа должна обладать следующими параметрами: • иметь графический интерфейс • возможность отследить выполнения каждого шага алгоритма Студент должен пояснить, каждый шаг алгоритма
2. Запрограмируйте на одном из языков программирования алгоритм вычисления хэш функции SHA-1	Программа должна обладать следующими параметрами: • иметь графический интерфейс • возможность отследить выполнения каждого шага алгоритма Студент должен пояснить, каждый шаг алгоритма

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:**	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения.

	шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	2 балла – студент полностью разобрался в решении задачи
2	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
3	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
1	**Знать:** наиболее известные системы псевдослучайных генераторов; **Уметь:** шифровать информацию с помощью различных криптосистем поточного шифрования **Владеть:** навыками вычисления хэш функций.	0 баллов – студент полностью неверно решил задачу 1 балл – студент написал программу, но не выполнил хотя бы одного из обязательных условий 2 балла – студент полностью разобрался в решении задачи
2	**Знать:** наиболее известные системы псевдослучайных генераторов; **Уметь:** шифровать информацию с помощью различных криптосистем поточного шифрования **Владеть:** навыками вычисления хэш функций.	0 баллов – студент полностью неверно решил задачу 1 балл – студент написал программу, но не выполнил хотя бы одного из обязательных условий 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 2 баллов (хотя бы по одной из компетенций)— оценка «неудовлетворительно», компетенция не сформирована;
- от 2 до 3 баллов (по) и 2 балла по — оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 4 до 5 баллов (по) и 2-3 балла (по) — оценка «хорошо», продвинутый уровень формирования компетенции;
- 6 баллов (по) и 4 балла (по) — оценка «отлично», высокий уровень формирования компетенции

Пример заданий для самостоятельной работы к разделу 5
Формируемая компетенция:

<table>
<tr><td>Задания</td><td>Ответы:</td></tr>
<tr><td>1. Есть три пользователя и используя протокол DIFFIE-HELLMAN сгенерируйте общий секретный ключ</td><td>Числовые значения могут отличаться от тех, которые приведены в данном решении
1.Пользователи и выбирают в открытом доступе большое простое число и . Пусть и 
2. Пользователь выбирает случайное большое натуральное число и отправляет пользователю 
величину ;
Пусть  и
3. Пользователь выбирает случайное большое натуральное число и отправляет пользователю 
величину  ;
Пусть  и
4. Пользователь выбирает случайное большое натуральное число и отправляет пользователю
величину  ;
Пусть и
5. Пользователь отправляет пользователю следующую величину ; Вычисляем
 
6. Пользователь отправляет пользователю следующую величину ; Вычисляем

7. Пользователь отправляет пользователю следующую величину ; Вычисляем
 
8. Пользователь вычисляет величину ;

Вычисляем
9. Пользователь вычисляет величину .

Вычисляем
10. Пользователь вычисляет величину .

Вычисляем

Получили</td></tr>
<tr><td>2.Опишите протокол с централизованным распределением ключей (протокол Цербера)</td><td>Для выработки сеансового ключа нужно выполнить следующие действия:
<table><tr><td>Символьная запись</td><td>Пояснения</td></tr><tr><td>1. </td><td>Пользователь сообщает , что хотел бы связаться с </td></tr><tr><td>2. , где
 - идентификатор пользователя ,
 - идентификатор пользователя ,
 - временная метка,
 - время жизни ключа</td><td>Доверенное лицо создает сообщение и передает его для передачи . Пользователь получает копию ключа в форме, которую он может прочесть.</td></tr><tr><td>3. </td><td>Пользователь , получив , легко может найти ключ . Клиент , желая проверить возможность общения с , посылает зашифрованную временную метку </td></tr><tr><td></td><td>Проверив, что временная метка является свежей, пользователь отправляет временную метку , показывая, что готов к сеансу.</td></tr></table></td></tr>
<tr><td>3. Есть два</td><td>Числовые значения могут отличаться от тех, которые приведены в данном решении</td></tr>
</table>

пользователя A и B используя протокол MTI сгенерируйте общий секретный ключ, если известно, что $n=17$	1.Пользователи A и B выбирают в открытом доступе большое простое число n и g, где g образующ элемент мультипликативной группы Z_n^* Пусть $n=17$ и 2. Пользователи A и B должны сгенерировать секретные ключи $1 \le x_A, x_B \le n-2$ и соответственно, и публикуют свои открытые ключи $y_A = g^{x_A} \bmod n$ и $y_B = g^{x_B} \bmod n$; Пусть Пользователь A генерирует число $x_A = 3$ и публикует $y_A = 3^3 \bmod 17 = 9$, соответственно пользо B генерирует число $x_B = 5$ и публикует $y_B = 3^5 \bmod 17 = 10$; 3. Пользователь A выбирает случайное натуральное число k_A, $1 \le k_A \le n-2$ и отправляет пользователю величину $X = g^{k_A} \bmod n$; Пусть пользователь A генерирует число $k_A = 4$ и отправляет пользователю B величину $X = 3^4 \bmod 17$ 4. Пользователь B выбирает случайное большое натуральное число k_B, $1 \le k_B \le n-2$ и отправляет пользователю A величину $Y = g^{k_B} \bmod n$; Пусть пользователь B генерирует число $k_B = 5$ и отправляет пользователю величину $Y = 3^5 \bmod 17 = 5$ 5. Пользователь A вычисляет величину $k = Y^{x_A} y_B^{k_A} \bmod n$; Пусть пользователь A на настоящий момент знает величины: $n, g, e, x_A, y_A, y_B, X, Y$. Пользователь A вычисляет величину $k = (Y^{x_A} y_B^{k_A}) \bmod n = (5^3 10^4) \bmod 17 = (15 * 10000) \bmod 17 = 15$ 6. Пользователь B вычисляет величину $k = X^{x_B} y_A^{k_B} \bmod n$. Пусть пользователь B на настоящий момент знает величины: $n, g, x_B, y_A, y_B, X, Y$. Пользователь B вычисляет величину $k = (X^{x_B} y_A^{k_B}) \bmod n = (13^5 9^5) \bmod 17 = (2197 * 59049) \bmod 17 = 15$ Получили $k = k = 15$
4. Опишите протокол Шамира	Протокол Шамира, позволяет пользователям A и B безопасно обмениваться информацией P без использования какой-либо общей секретной информации. Он предполагает использование коммутатив симметричного шифра, для которого: $E_{k_A}(E_{k_B}(P)) = E_{k_B}(E_{k_A}(P))$, где E -шифрующее преобразование, k_A - секретный ключ пользователя A, а k_B - секретный ключ пользователя B. Тогда трехпроходный протокол Шамира для передачи ключа k от A к B может быт реализован следующим образом

Символьная запись	Пояснения
1. $A \to B: \; E_{k_A}(k)$	Пользователь A шифрует ключ k и передает результа пользователю B
2. $B \to A: \; E_{k_B}(E_{k_A}(k))$	Пользователь B шифрует полученное сообщение и пер результат пользователю A
3. $A \to B: \; D_{k_A}(E_{k_B}(E_{k_A}(k)))$, где D -дешифрующее преобразование	Пользователь A дешифрует полученное сообщение и передает результат пользователю B. В результате у пользователя B остается сообщение $E_{k_B}(k)$, которое с легко может дешифровать.

Критерии оценивания

Номер задачи	Критерии	Шкала оценивания
1	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения.

	криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	2 балла – студент полностью разобрался в решении задачи
2	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	0 баллов – студент полностью неверно решил задачу 2 балла – студент полностью разобрался в решении задачи
3	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	0 баллов – студент полностью неверно решил задачу 1 балл – студент верно решил задачу, но не привел пояснений к ходу решения. 2 балла – студент полностью разобрался в решении задачи
4	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	0 баллов – студент полностью неверно решил задачу 2 балла – студент полностью разобрался в решении задачи

Набранное количество баллов соответствует оценке за выполнение работы:
- менее 4 баллов— оценка «неудовлетворительно», компетенция не сформирована;
- от 4 до 5 баллов— оценка «удовлетворительно», пороговый уровень формирования компетенции;
- от 5 до 7 баллов— оценка «хорошо», продвинутый уровень формирования компетенции;
- 8 баллов— оценка «отлично», высокий уровень формирования компетенции

1.2.Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы для подготовки к зачету во 2 семестре.
На зачете проверяется сформированность знаний, умений и навыков в соответствии с компетенциями , и .
Зачет проводится в устной форме и выставляется по итогам ответов, данных студентом на два вопроса из списка. Список вопросов к зачету заранее доступен для студентов (студент должен выполнить все самостоятельные работы).

1. Понятие математической защиты информации и информационной безопасности
2. Способы защиты информации.
3. Некоторые исторические алгоритмы (алгоритмы Цезаря, Виженера).
4. Криптоанализ исторических алгоритмов (алгоритмы Цезаря, Виженера).

5. Влияние длины блока на криптографическую стойкость алгоритма (алгоритмы Хилла и Плейфейра).

6. Ассиметричная криптосистема: рюкзачная криптосистема и ее криптоанализ.

7. Ассиметричная криптосистема: плотный рюкзак.

8. Крптосистема RSA и ее криптоанализ.

9. Криптосистемы основанные на дискретных логарифмах.

10. Криптосистемы Рабина, Эль-Гамеля.

11. Криптосистема Вильемса, Уильямса

12.Обзор потоковых кодов.

13. Симметричные криптосистемы (алгоритмы DES, Blowfish, Гост28147-89, AES, RC6, Serpent, Mars).

Критерии оценивания

Оценка **«зачтено»** выставляется студенту, который:

- прочно усвоил предусмотренный программный материал;
- правильно, аргументировано ответил на все вопросы, с приведением примеров;
- показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов.

Дополнительным условием получения оценки «зачтено» могут стать хорошие успехи при выполнении самостоятельных работ, систематическая активная работа на занятиях.

Оценка **«не зачтено»** Выставляется студенту, который не справился с 50% вопросов и заданий, в ответах на другие вопросы допустил существенные ошибки. Не может ответить на дополнительные вопросы, предложенные преподавателем. Целостного представления о взаимосвязях, компонентах дисциплины у студента нет.

Вопросы для подготовки к зачету .

На зачете проверяется сформированность знаний, умений и навыков в соответствии с компетенциями и .

Зачет проводится в устной форме и выставляется по итогам ответов, данных студентом на два вопроса из списка. Список вопросов к зачету заранее доступен для студентов (студент должен выполнить все самостоятельные работы).

1. ЭЦП RSA, ЭЦП Эль-Гамаля.

2. Схема ЭЦП DSA и ее модификация.

3. Схема ГОСТ Р34.10-94 и ее модификация.

4. Подделка ЭЦП. Неотрицаемые цифровые подписи

5. Криптосистемы основанные на эллептических кривых.

6. Свойства криптографических хэш-функций. Их использование в протоколах аутентификации и для контроля изменения чувствительной информации. Однонаправленные хэш-функции, использующие симметричные блочные алгоритмы.

7. Хэш-функция MD5

8. Хэш-функция SHA-1

9. Распределение ключей. Трехпроходный протокол Шамира.

10. Открытое распределение ключей

11.Обмен зашифрованными ключами: базовый протокол EKE (реализация EKE с помощью RSA, Эль-Гамаля, Diffie-Hellman.)

12. Разделение секрета. Схема интерполяционных многочленов Лагранжа.

13. Подсознательный канал (Ong-Schnorr-Shamir, Эль-Гамаль, DSA).

14. Доказательство с нулевым знанием.

Критерии оценивания

Оценка **«зачтено»** выставляется студенту, который:

- прочно усвоил предусмотренный программный материал;
- правильно, аргументировано ответил на все вопросы, с приведением примеров;
- показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов.

Дополнительным условием получения оценки «зачтено» могут стать хорошие успехи при выполнении самостоятельных работ, систематическая активная работа на занятиях.
Оценка **«не зачтено»** Выставляется студенту, который не справился с 50% вопросов и заданий, в ответах на другие вопросы допустил существенные ошибки. Не может ответить на дополнительные вопросы, предложенные преподавателем. Целостного представления о взаимосвязях, компонентах дисциплины у студента нет.

2. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

2.1 Шкала оценивания сформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующей трехуровневой шкале:

Пороговый уровень - предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков, полученных аспирантом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для аспиранта к моменту завершения им освоения данной дисциплины.

Продвинутый уровень - предполагает способность аспиранта использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень по нескольким существенным признакам,

в том числе по наличию более широких знаний о классических и основных теориях информации; углублённых знаний о принципах формирования и реализации информационных процессов; умению применять современные информационные технологии для поиска и обработки актуальной информации, демонстрацию владения современными моделями СППР и навыками программирования при решении социально значимых задач.

Высокий уровень - предполагает способность аспиранта использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профессиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям.
Высокий уровень превосходит пороговый уровень по всем существенным признакам,

2.2 Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования

Планируемые результаты Обучения	Критерии оценивания результатов обучения		
	Пороговый уровень	**Продвинутый уровень**	**Высокий уровень**
Знать: наиболее известные симметричные криптосистемы; **Уметь:** шифровать информацию с помощью различных симметричных криптосистем; **Владеть** навыками построения модели информационной безопасности.	**Знать:** наиболее известные симметричные криптосистемы;	**Знать:** наиболее известные симметричные криптосистемы; **Уметь:** шифровать информацию с помощью различных симметричных криптосистем;	**Знать:** наиболее известные симметричные криптосистемы; **Уметь:** шифровать информацию с помощью различных симметричных криптосистем (программировать); **Владеть** навыками построения модели информационной безопасности.
Знать: наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа **Владеть** навыками создавать ЭЦП; навыками работы с ключами.	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа (RSA, Эль-Гамаля) **Владеть** навыками создавать ЭЦП (RSA, Эль-Гамаля);	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа (RSA, Эль-Гамаля, Уильемса, Вильемса) **Владеть** навыками создавать ЭЦП (RSA, Эль-Гамаля,DSA)	**Знать:** наиболее известные криптосистемы открытого ключа; **Уметь:** шифровать информацию с помощью различных криптосистем открытого ключа (RSA, Эль-Гамаля, Уильемса, Вильемса, Плотный рюкзак) **Владеть** навыками создавать ЭЦП (RSA, Эль-Гамаля,DSA,Гост)
Знать: наиболее известные системы	**Знать:** наиболее известные системы	**Знать:** наиболее известные системы псевдослучайных генераторов	**Знать:** наиболее известные системы псевдослучайных генераторов (Конгруэнтные генераторы и их

псевдослучайных генераторов; **Уметь:** шифровать информацию с помощью различных криптосистем поточного шифрования **Владеть:** навыками вычисления хэш функций.	псевдослучайных генераторов; **Уметь:** шифровать информацию с помощью различных криптосистем поточного шифрования .	(Конгруэнтные генераторы, Регистры сдвига LFSR, Аддитивные генераторы) **Уметь:** шифровать информацию с помощью различных криптосистем поточного шифрования	криптоанализ, Регистры сдвига LFSR и их криптоанализ. Аддитивные генераторы) **Уметь:** шифровать информацию с помощью различных криптосистем поточного шифрования **Владеть:** навыками вычисления хэш функций(MD5, SHA-1).

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения аспирантом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения аспирантом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе 1.«Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1 Критерии оценивания степени овладения знаниями¸ умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

- достаточно полные и систематизированные знания в объёме программы дисциплины;

- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

- систематизированные, глубокие и полные знания по всем разделам дисциплины;
- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Оценивание результатов обучения студентов по дисциплине «Информатика» осуществляется по регламенту текущего контроля и промежуточной аттестации.

Текущий контроль в семестре проводится с целью обеспечения своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы студентов.

Текущий контроль проводится в виде практических и творческих работ.

Оценка сформированности компетенций при итоговом уровняе аттестации

оценка	**уровень**
зачтено	высокий, продвинутый, пороговый
незачтено	Не сформирован

Приложение №2 к рабочей программе дисциплины
«Математические основы защиты информации и информационной безоспасности»

Методические указания для аспирантов по освоению дисциплины

Формы преподавания дисциплины «Математические методы защиты информации и информационной безопасности» достаточно традиционны. Это лекции, как наиболее эффективный по времени путь передачи большого объема материала большой группе обучающихся. Как правило, аспиранты записывают в свои конспекты излагаемый на доске материал. Составление конспекта лекций и дальнейшая работа с ним при подготовке к занятиям выступает как значительная часть процесса обучения. Практические занятия обычно с лекциями дополняют друг друга. Проводятся в академических группах под руководством преподавателя. Основной целью является формирование у аспирантов понимания теоретического материала, изложенного на лекции, через решение упражнений и задач. Здесь преподавание строится на разумном для каждой темы сочетании коллективной работы группы с самостоятельной индивидуальной работой аспирантов. Допустима также работа в небольших группах по обсуждению серии взаимосвязанных вопросов обучаемым и коллективного поиска ответов на них.

Домашние задания подразделяются на текущие (задание к очередному практическому занятию или лекции) и долгосрочные, т.е. задания выдаются на длительный период с обязательным предъявлением результатов. К последним относятся задания, связанные с реализацией моделей на компьютере. Аспиранты регулярно получают задания по самостоятельному изучению некоторых вопросов курса, а также дополнительных его разделов, по чтению учебной литературы.

Групповые консультации проводятся перед контрольными мероприятиями (контрольные работы, зачетные работы, экзамены) для большой группы аспирантов с целью систематизации знаний и устранению имеющихся сложностей с пониманием материала общего характера.

Самостоятельная работа реализуется:

1. Непосредственно в процессе аудиторных занятий.
2. В контакте с преподавателем вне рамок расписания - на консультациях по учебным вопросам, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.
3. В библиотеке, дома, и т.д. при выполнении аспирантом учебных задач.

Перенос активности аспирантов на работу во внеаудиторное время связан с рядом трудностей, основная из которых - это неготовность к нему большинства аспирантов, особенно младших курсов. Поэтому на практических занятиях преподаватель старается приучить аспиранта работать самостоятельно, отводя для этого около половины времени на самостоятельное решение задач. Практические занятия строятся следующим образом:

1. Формулировка целей занятия, основных вопросов, которые должны быть рассмотрены.
2. Опрос.
3. Решение нескольких типовых задач у доски.
4. Самостоятельное решение задач.

5. Разбор ошибок при решении (в конце текущего занятия или в начале следующего).
По результатам самостоятельного решения задач и по проверке подготовки аспиранта к практическому занятию (письменный опрос по теории и проверка домашнего задания) аспирант получает оценку. По материалам темы проводится контрольная работа. Результаты выполнения этих заданий формируют оценку работы аспиранта в конце семестра, которая составляет часть итоговой оценки на экзамене.

Учебно-методическое обеспечение
самостоятельной работы аспирантов по дисциплине

Для самостоятельной работы рекомендуется использовать учебную литературу:

а) основная литература:

1. Нестеров, С. А., Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров, М., Юрайт, 2016, 321с
2. Нестеров, С. А., Информационная безопасность [Электронный ресурс] : учебник и практикум для академического бакалавриата / С. А. Нестеров, М., Юрайт, 2017, 321с
https://biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7/informacionnaya-bezopasnost

б) дополнительная литература:

1. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493175 (16.01.2019).
2. В.И. Аверченков Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Издательство «Флинта», 2016. - 224 с. [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93351 .
3.Ш.Т. Ишмухаметов Математические основы защиты информации: Электронное учебное пособие для студентов института вычислительной математики и информационных технологий / Ш.Т. Ишмухаметов, Р.Г. Рубцова. - Казань: Казанский федеральный университет, 2012. - 138 с. [Электронный ресурс]. - URL: http://window.edu.ru/resource/128/78128/files/mzi.pdf
4. Внуков, А. А. Защита информации : учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. —[Электронный ресурс]. https://biblio-online.ru/viewer/zaschita-informacii-414082

5. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Издательство Юрайт, 2018. — 473 с. — (Серия : Бакалавр. Академический курс). —[Электронный ресурс]. https://biblio-online.ru/viewer/kriptograficheskie-metody-zaschity-informacii-413075

Для самостоятельной работы особенно рекомендуется использовать учебную литературу.
Также для подбора учебной литературы рекомендуется использовать широкий спектр интернет-ресурсов:

1. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru) - электронная библиотека, обеспечивающая доступ к наиболее востребованным материалам-первоисточникам, учебной, научной и художественной литературе ведущих издательств (*регистрация в электронной библиотеке – только в сети университета. После регистрации работа с системой возможна с любой точки доступа в Internet.).

2.Информационная система "Единое окно доступа к образовательным ресурсам" (http://window.edu.ru/library).
Целью создания информационной системы "Единое окно доступа к образовательным ресурсам" (ИС "Единое окно ") является обеспечение свободного доступа к интегральному каталогу образовательных интернет-ресурсов и к электронной библиотеке учебно-методических материалов для общего и профессионального образования.
Информационная система "Единое окно доступа к образовательным ресурсам" создана по заказу Федерального агентства по образованию в 2005-2008 гг. Головной разработчик проекта - Федеральное государственное автономное учреждение Государственный научно-исследовательский институт информационных технологий и телекоммуникаций (ФГАУ ГНИИ ИТТ "Информика") www.informika.ru.

Для самостоятельного подбора литературыв библиотеке ЯрГУ рекомендуется использовать:
1. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php)дает возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню «Электронный каталог»; пройти процедуру авторизации, выбрав вкладку «Авторизация», и заполнить представленные поля информации.
2. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.
3. Электронная картотека «Книгообеспеченность» (http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php) раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.