




МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДФУ)

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

СОГЛАСОВАНО

Руководитель ОП

 Гузев М.А.
(подпись) (ФИО)

«УТВЕРЖДАЮ»

 Директор департамента
Сущенко А.А.
(подпись) (ФИО)
« 25 » марта 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы теории кодирования

Направление подготовки 09.03.03 Прикладная информатика

(Прикладная информатика в компьютерном дизайне)

Форма подготовки очная

курс 3 семестр 6

лекции 18 час.

практические занятия не предусмотрены

лабораторные работы 18 час.

в том числе с использованием МАО лек. / пр. - / лаб. 18 час.

всего часов аудиторной нагрузки 36 час.

в том числе с использованием МАО 18 час.

самостоятельная работа 72 час.

в том числе на подготовку к экзамену час.

контрольные работы (количество) не предусмотрены

курсовая работа / курсовой проект не предусмотрены

зачет 6 семестр

экзамен семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 09.03.03 Прикладная информатика утвержденного приказом Министерства образования и науки РФ от 19 сентября 2017 г. № 922 (с изменениями и дополнениями).

Рабочая программа обсуждена на заседании кафедры информатики, математического и компьютерного моделирования протокол №10 от « 25 » марта 2022г.

Директор департамента математического и компьютерного моделирования Сущенко А.А.

Составители: ст.преподаватель, Серга И.В.

Владивосток
2022

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании департамента:

Протокол от « ____ » _____ 20__ г. № ____

Директор департамента _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании департамента:

Протокол от « ____ » _____ 20__ г. № ____

Директор департамента _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании департамента:

Протокол от « ____ » _____ 20__ г. № ____

Директор департамента _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании департамента:

Протокол от « ____ » _____ 20__ г. № ____

Директор департамента _____
(подпись) (И.О. Фамилия)

АННОТАЦИЯ

Рабочая программа учебной дисциплины «Криптография» разработана для студентов 4 курса, обучающихся по направлению 09.03.03 «Прикладная информатика».

При изучении дисциплины охватывается следующий круг вопросов: докомпьютерная криптография, блочно-итеративные криптосистемы, криптосистемы с открытым ключом, современные подходы к защите информации.

В процессе изучения данного курса студенты должны овладеть базовыми знаниями в области криптологии и усовершенствовать свои навыки в решении прикладных математических задач, в разработке алгоритмов и реализации их в виде программ, а также в анализе текстов с описанием алгоритмов и документации к программным системам и утилитам. В результате изучения данного курса студенты должны приобрести навыки и умения, расширить эрудицию в области современных информационных технологий, но также познакомиться с некоторыми социальными функциями информатики.

Данный УМКД содержит некоторые материалы, которые представлены на странице курса, размещенной в Интернет и предназначенной для использования студентами в процессе обучения. Приведен перечень основных тем, излагаемых на лекциях, а также тексты задач, в процессе решения которых студенты вырабатывают и совершенствуют навыки и умения, необходимые для будущей профессиональной деятельности в сфере информационных технологий.

Курс включает в себя следующие основные темы

- Классическая криптография.
- Основы теории информации Шеннона.
- Блочные симметричные итеративные шифры.
- Элементы теории сложности.
- Системы с открытым ключом.
- Первообразные корни и их свойства.
- Протокол взаимной аутентификации.

- Современные криптографические протоколы для обеспечения секретности и идентификации.
- Квантовая криптография.

В рамках этого курса демонстрируется применение математических методов к формированию алгоритмов и протоколов, связанных с защитой информации. В курсе используются навыки и умения, полученные на предыдущих стадиях подготовки в рамках таких предметов, как дискретная математика, алгебра, теория вероятностей, языки программирования.

Цель изучения курса является освоение математических основ криптологии и принципов защиты информации при ее хранении, обработке и передаче, а также совершенствование навыков решения задач с использованием компьютера.

Задачи:

4. Изучение математических основ криптологии.
5. Выработка умений для анализа и реализации в виде программного обеспечения алгоритмов и протоколов, используемых при защите информации.
6. Формирование представлений о роли информационных технологий в жизни общества.

Тип задач	Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
Проектный	ПК-7 Способен проводить научно-исследовательские и опытно-конструкторские разработки в области цифровизации предприятий	ПК-7.1 Демонстрирует знание методологий науки и техники, методов исследования объектов профессиональной деятельности и разработки моделей, способов обеспечения качества исследований и требований стандартов по оформлению научно-исследовательских отчетов
		ПК-7.2 Исследует объекты профессиональной деятельности, выявляет и идентифицирует актуальные проблемы, предлагает гипотезы, формирует цели и задачи

		<p>исследований и разработки, осуществляет сбор и обработку результатов проектных исследований, предлагает варианты решений, осуществляет выбор, составляет отчеты о проделанной работе, обзоры</p>
		<p>ПК-7.3 Разрабатывает модели объектов профессиональной деятельности, осуществляет оценку полученного результата, определяет качество проводимых исследований, составляет отчеты о проделанной работе, обзоры, готовит публикации</p>
Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)	
<p>ПК-7.1 Демонстрирует знание методологий науки и техники, методов исследования объектов профессиональной деятельности и разработки моделей, способов обеспечения качества исследований и требований стандартов по оформлению научно-исследовательских отчетов</p>	<p>Знать: методологии науки и техники, методов исследования объектов профессиональной деятельности и разработки моделей, способов обеспечения качества исследований и требований стандартов по оформлению научно-исследовательских отчетов, исследования объектов профессиональной деятельности.</p>	
	<p>Уметь: использовать методологии науки и техники, методов исследования объектов профессиональной деятельности.</p>	
	<p>Владеть: навыками использования знаний естественнонаучных дисциплин, вычислительной техники и программирования для решения общих задач естествознания, техники, навыками применения знаний к теоретически и практическим исследованиям</p>	
<p>ПК-7.2 Исследует объекты профессиональной деятельности, выявляет и идентифицирует актуальные проблемы, предлагает гипотезы, формирует цели и задачи исследований и разработки, осуществляет сбор и обработку результатов проектных исследований, предлагает варианты решений, осуществляет выбор, составляет отчеты о проделанной работе, обзоры</p>	<p>Знать: основы профессии, принципы архитектуры вычислительной техники и системы программного обеспечения; программную инженерию, технологии программирования и способы реализации программных проектов.</p>	
	<p>Уметь: корректно ставить профессиональные задачи; использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач; самостоятельно проводить анализ результатов научно-исследовательской работы, делать обоснованные выводы.</p>	
	<p>Владеть: способностью использовать профессиональные методы при анализе проблем в области профессиональной деятельности; способностью участвовать в создании информационных и компьютерных систем, программных проектов на всех этапах жизненного</p>	

	цикла.
ПК-7.3 Разрабатывает модели объектов профессиональной деятельности, осуществляет оценку полученного результата, определяет качество проводимых исследований, составляет отчеты о проделанной работе, обзоры, готовит публикации	Знать: определения и свойства основных объектов профессиональной деятельности
	уметь: решать задачи вычислительного и теоретического характера, находить оптимальные решения с наименьшим риском ошибки.
	владеть: разнообразным профессиональным разработкой, описания и оценки моделей объектов профессиональной деятельности

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекции (18 часов)

Раздел I. Докомпьютерная криптография (6/36)

- Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Поточковые и блочные шифры.
- Докомпьютерная криптография . Шифры *Виженера*. Автоматический и бегущий выбор ключа.
- Шифры Вернама, Плейфейера, Хилла. Шифр одноразового блокнота.
- Энтропия и информация по Шеннону. Условие абсолютной криптостойкости шифра.

Раздел II. Блочные симметричные итеративные шифры (6/36)

- Шифр Файстеля. Структура шифра. Алгоритм дешифрования. Диффузия и конфузия.
- DES: шифрование и дешифрование. Лавинный эффект. Надежность. Криптоанализ.
- Режимы работы DES. Сцепление блоков. Шифрованная обратная связь. Двойной и тройной DES. Другие симметрично-блочные шифры.

Раздел III. Элементы теории сложности вычислений (4/36)

- Классы языков. Временная сложность вычислений. Классы P и NP. Примеры NP-трудных проблем. Языки составных и простых чисел.

Раздел IV. Криптосистемы с открытым ключом (10/36)

- Криптосистемы, базирующиеся на задаче о рюкзаке.
- Группы, кольца, области целостности, поля. Классы вычетов по модулю.
- Простые числа. Основная теорема арифметики. Теорема Евклида о существовании бесконечного множества простых чисел. Теорема о промежутках между простыми числами.
- Малая теорема Ферма. Теорема Эйлера.
- RSA: основные элементы криптосистемы. Шифрование и дешифрование.
- Греко-китайская теорема об остатках и ее применения.
- Возведение в степень с использованием метода последовательного возведения в квадрат.
- Теорема о корнях $x^2=1 \pmod p$ для нечетного простого p . Рандомизация проверки простоты (WITNESS). Числа Карлмайкла.

Раздел V. Аутентификация (6/36)

- Первообразные корни и их свойства. Дискретные логарифмы.
- Протокол взаимной аутентификации. Схема обмена ключами Диффи-Хеллмана.

Раздел VI. Современные проблемы (4/36)

- Квантовая криптография.
- Доказательства без разглашения, протоколы электронного голосования, неотслеживаемость транзакций, разделение секретов и т. д.

Источники:

1. Brassar Ж. Современная криптология. - М.: Полимед, 1999. Введение в криптографию /Под общ.ред. В.В. Яценко. - М.: МЦНМО: "ЧеРо", 1999. Brassar Ж. Современная криптология. - М.: Полимед, 1999.
2. Richard E. Blahut Cryptography and Secure Communication. Cambridge University Press, 2014.
3. Jonathan Katz, Yehuda Lindell Introduction to Modern Cryptography: Principles and Protocols, Chapman and Hall CRC, 2007.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

На лабораторных и практических работах проводится обсуждение и сдача решений задач, которые выдаются в процессе лекций. Также на лабораторных работах проводится обсуждение рефератов.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Рекомендации по самостоятельной работе студентов

Самостоятельная работа студентов состоит из решения задач и подготовки реферата по согласованной теме.

Рефераты

Реферат объемом 2 стр. без обложки должен быть представлен и защищен до экзамена/зачета по согласованной теме (темы, предварительный список литературы и содержание для согласования нужно присылать по почте). Основное направление -- криптоанализ и отдельные составляющие изученных систем, а также современные криптографические протоколы, криптографические системы и т. п., которые не были затронуты на лекциях. Требуется подобрать и изучить современные источники и попытаться на двух стр. самостоятельно изложить материал со ссылками на библиографические описания использованных источников. Любое заимствование должно быть явно обозначено. Примеры рефератов, подготовленных в предыдущие годы, доступны на сайте (Алгоритм шифрования IDEA, Коллизии хэш-функций, Схема разделения секрета Шамира, протоколы для обеспечения секретности и идентификации и т. д.).

Основные требования к содержанию реферата

Студент должен использовать только те материалы (научные статьи, монографии, пособия), которые имеют прямое отношение к избранной им теме.

По своей *структуре* реферат состоит из:

1. Введения, где студент формулирует проблему, подлежащую анализу и исследованию;

2. Основного текста, в котором последовательно раскрывается избранная тема. Возможно описание фрагментов кода, который разрабатывается в процессе подготовки реферата.

3. Заключение, где студент формулирует выводы, сделанные на основе основного текста.

4. Списка использованной литературы. В данной список включаются все источники, на которые имеются ссылки в тексте. Использование материалов Википедии является нежелательным.

Порядок сдачи реферата и его оценка

Реферат готовится студентами в течение семестра по тематике, согласуемой по почте. Защита рефератов проводится в рамках лабораторных работ. При защите реферата студент должен дать разъяснения и ответить на вопросы по тексту.

Тематика рефератов

1. Альтернативные системы с открытым ключом
2. Системы, базирующиеся на использовании эллиптических кривых
3. Протоколы для голосования
4. Разделение секретов

Задачи для самостоятельного решения

1. Докомпьютерная криптография: Показать, что $\text{НОД}(a, |A|) = 1$ н. и д. для однозначности дешифрования шифра $c = a * m + b \pmod{|A|}$.
2. Докомпьютерная криптография: Описать обратное преобразование для модулярного шифра с $a \neq 1$. Будет ли оно модулярным шифром?
3. Докомпьютерная криптография: Сколько всего различных модулярных шифров в $|A|$ -буквенном алфавите A (вывести формулу)? Посчитать по формуле для английского языка, где $|A|=26$.
4. Докомпьютерная криптография: Сколько возможных ключей позволяет использовать шифр Плейфейера? (Представить приблизительно в виде степени двойки.)

5. Докомпьютерная криптография: Реализовать (Scheme, Mathematica, Sage, ...) схему шифрования-дешифрования Плейфейера, подготовить тесты по методу белого ящика, продемонстрировать его работу и методику криптоанализа на достаточно длинном зашифрованном тексте.

6. Докомпьютерная криптография: Расшифровать заданное сообщение `ymjkwjvzjshdrjymtisjjixqt slhnumjwujsuxybtwtp` с использованием частотной таблицы (модулярный шифр с $n=1$).

7. Докомпьютерная криптография: Реализовать программу (Scheme, Mathematica, Sage, ...) для подсчета частоты встречаемости отдельных символов, пар, троек и т.д. Подготовить тесты. Продемонстрировать работу на достаточно длинном тексте. Сравнить результаты с известными.

8. Докомпьютерная криптография: Описать и реализовать (Scheme, Mathematica, Sage, ...) методику криптоанализа шифра Виженера (продемонстрировать методику криптоанализа на достаточно длинном зашифрованном тексте).

9. Докомпьютерная криптография: Каким необходимым и достаточным условиям должен удовлетворять определитель матрицы E для того, чтобы преобразование Хилла $c = E \cdot m + s \pmod{|A|}$, c, m, s - n -мерные векторы, E - $n \times n$ -матрица, обладало свойством взаимной однозначности?

10. Докомпьютерная криптография: Какие из изученных докомпьютерных шифров являются групповыми, а какие нет (с доказательством)?

11. Докомпьютерная криптография: Показать, что шифр перестановки является линейным преобразованием в V^n , $V = \{0, 1\}$.

12. Докомпьютерная криптография: Сколько существует нелинейных криптопреобразований $V^3 \rightarrow V^3$?

13. Докомпьютерная криптография: Доказать, что энтропия скалярного источника дискретных сообщений, заданного вероятностями p_1, \dots, p_n , принимает максимальное значение т. и т. т., когда все p_i , $i=1, \dots, n$, совпадают.

(Известно, что если некоторая функция h_n от p_1, \dots, p_n непрерывна по совокупности переменных и обладает дополнительно тремя свойствами: 1) ее максимум достигается при равных $p_i, i=1, \dots, n$, 2) иерархической аддитивности, 3) добавление к алфавиту еще одного символа с нулевой вероятностью не меняет ее значения, т.е.

$h_{n+1}(p_1, \dots, p_n, 0) = h_n(p_1, \dots, p_n)$, то h_n необходимо имеет вид шенноновской энтропии: $h_n(p_1, \dots, p_n) = -\lambda \sum_{i=1}^n p_i \log p_i$, где $\lambda > 0$).

14. Докомпьютерная криптография: Доказать свойство иерархической аддитивности для векторного источника дискретных сообщений.

15. Применение теории информации: Какая информация будет получена в результате проведения зачета, если студент получает зачет с вероятностью 0.9, если он готовился, и 0.3, если нет, и известно, что 90% студентов готовились к зачету.

16. Докомпьютерная криптография: Для абсолютно криптостойкой системы $I(\phi, \xi) = I(\xi, \phi) = 0$: информация об исходном тексте в открытом (зашифрованном) равна нулю.

17. Блочные симметричные итеративные шифры: Реализовать DES с использованием Scheme, Mathematica, Sage, ... и протестировать программу с использованием материалов со страницы [Ronald R. Testing implementations of DES](#).

18. Блочные симметричные итеративные шифры: Разработать программы и тесты для демонстрации различных режимов использования DES (Scheme, Mathematica, Sage, ...).

19. Блочные симметричные итеративные шифры : Доказать свойство дополненности DES (1): если $C = \text{DES}(M, K)$, то $C' = \text{DES}(M', K')$ (Z' - обозначает слово, составленное из дополнений соответствующих битов бинарного слова Z). (Используйте следующее равенство для логических переменных $(x+y)' = x'+y'$).

20. Блочные симметричные итеративные шифры: Продемонстрировать лавинный эффект в DES: написать программу (Scheme, Mathematica, Sage), которая вычисляет расстояние Хемминга для результатов раундовых преобразований при изменении одного бита в исходном сообщении и в ключе. Для этого сгенерировать сообщение и ключ, а затем, изменив в сообщении ровно один бит случайным образом, рассчитать расстояние Хемминга между результатами раундовых преобразований. Вычислить также среднее расстояние по набору исходных сообщений для всех 16 раундов. Аналогичные действия проделать для фиксированного сообщения и изменений одного бита ключа.

21. Криптосистемы с открытым ключом: Доказать, что $n_i = 2^i$, $i=1, 2, \dots, 1$) является минимальной супервозрастающей последовательностью, 2) может использоваться для кодирования любого числа (при достаточно большом k), 3) никакая другая не обладает свойством 2.

22. RSA: Оценить вероятность того, что $0 < w < n$ будет не взаимно просто с $n=pr$. Показать, что и при $\text{НОД}(n,w) \neq 1$ расшифрование RSA сводится к возведению в степень d .

23. Пусть $p = P[\text{НОД}(a,b)=1]$, где a, b - два выбранные наугад числа].
- Доказать, что $P[\text{НОД}(a,b)=d]$, где a, b - два выбранные наугад числа] $= p/d^2$.
- Доказать, что $\sum_{d \geq 1} P[\text{НОД}(a,b)=d]$, где a, b - два выбранные наугад числа] $= 1$.
- Доказать, что p примерно равна 0.6.

24. Криптосистемы с открытым ключом: Исполнить WITNESS при $a=7$, $n=561$ и проинтерпретировать результат.

25. Криптосистемы с открытым ключом: Найти $(678 * 973) \bmod 1813$ (с использованием греко-китайской теоремы)

26. Криптосистемы с открытым ключом: Сгенерировать все компоненты RSA, протестировать кодирование/декодирование.

27. Криптосистемы с открытым ключом: Шесть профессоров начинают читать лекции по своим курсам в ПН, ВТ, СР, ЧТ, ПТ, СБ и читают их далее

через 2, 3, 4, 1, 6, 5 дней соответственно. Лекции не читаются по ВС (отменяются). На какой по порядку неделе в первый раз все лекции выпадут на ВС и будут отменены?

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

Вопросы к зачету / экзамену

- Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Поточковые и блочные шифры.
- Рандомизация проверки простоты (WITNESS). Числа Карлмайкла}
- Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Поточковые и блочные шифры.
- Протокол взаимной аутентификации. Схема обмена ключами Диффи-Хеллмана.
- Модулярные шифры. Шифры Виженера. Автоматический и бегущий выбор ключа.
- Теорема о корнях $x^2=1 \pmod p$ для нечетного простого p .
- Шифры Вернама, Плейфейера, Хилла. Шифр одноразового блокнота. Абсолютно криптостойкие шифры.
- Греко-китайская теорема об остатках и ее применения.
- Шифр Файстеля. Структура шифра. Алгоритм дешифрования.
- Малая теорема Ферма. Теорема Эйлера.
- DES: алгоритмы шифрования и дешифрования. Надежность.
- Криптоанализ. Диффузия и конфузия.
- Возведение в степень с использованием метода последовательного возведения в квадрат.
- Тройной DES.
- Группы, кольца, области целостности, поля.

- Двойной DES.
- Криптосистемы, базирующиеся на задаче о рюкзаке.
- Режимы работы DES. Сцепление блоков.
- Обмен ключами по алгоритму BB84 (квантовая криптография).
- Простые числа. Основная теорема арифметики. Теорема Евклида о существовании бесконечного множества простых чисел. Теорема о промежутках между простыми числами.
- RSA: основные элементы криптосистемы. Шифрование и дешифрование.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(печатные и электронные издания)

1. Теория информации и кодирование: учебное пособие: [учебное электронное издание]/ Кулешов Е. Л. – 2021.
<https://lib.dvfu.ru/lib/item?id=chamo:888756&theme=FEFU>
2. Криптографическая защита информации/ Крамаров С. О., Тищенко Е. Н., Соколов С. В., Шевчук П. С., Митясова О. Ю. – РИОР, 2021.
<https://lib.dvfu.ru/lib/item?id=Znanium:Znanium-1153156&theme=FEFU>
3. Дискретная математика. Сборник задач/ Гусева А. И., Киреев В. С., Тихомирова А. Н. – Курс, 2021. <https://lib.dvfu.ru/lib/item?id=Znanium:Znanium-1094740&theme=FEFU>
4. Математические и компьютерные основы криптологии. - Минск: ООО "Новое знание", 2003.
5. Саломаа А. Криптография с открытым ключом. М.: Мир, 1996.
6. Столлингс В. Криптография и защита сетей: принципы и практика. М.: Изд. дом Вильямс, 2003.
7. Акритас А. Основы компьютерной алгебры. М.: Мир, 1994.
8. Сمارт Н. Криптография. - Москва: Техносфера, 2005.
9. Брассар Ж. Современная криптология. - М.: Полимед, 1999.
10. Хопкрофт Дж., Ульман Дж., Мотвани Р. Введение в теорию автоматов, языков и вычислений. - М.: Изд. дом Вильямс, 2002.
11. Рябко Б. Я., Фионов А. Н. Защита информации. — 2-е изд. — М.: Горячая линия — Телеком, 2013.
12. Jonathan Katz, Yehuda Lindell Introduction to Modern Cryptography: Principles and Protocols, Chapman and Hall CRC, 2007.
13. Philip N. Klein A Cryptography Primer: Secrets and Promises. CambridgeUniversityPress, 2014.

14. Richard E. Blahut Cryptography and Secure Communication. CambridgeUniversityPress, 2014.

Дополнительная литература (печатные и электронные издания)

1. Осипян В. О., Осипян К. В. Криптография в упражнениях и задачах
Издательство: Гелиос АРВ, 2004.
2. Скембрей Дж, Мак-Клар С., Курц Дж. Секреты хакеров. Безопасность сетей
- готовые решения. М.: Изд. дом Вильямс, 2001.
3. Ноден П., Китте К. Алгебраическая алгоритмика (с упражнениями и
решениями). - М.: Мир, 1994
4. Введение в криптографию /Под общ.ред. В. В. Яценко. - М.: МЦНМО:
"ЧеРо", 1999.
5. Фергюсон Н., Шнайдер Б. Практическая криптография. -- М.: Вильямс,
2005.
6. Материалы, посвященные книге Столлингс В. "Криптография и защита
сетей: принципы и практика". <http://williamstallings.com/Crypto3e.html> (запрошен
01.09.2013).

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Процесс изучения дисциплины осуществляется в следующих организационных формах:

- лекционные занятия;
- выполнение аудиторных лабораторных работ;
- самостоятельное изучение материала;
- выполнение индивидуальных работ;
- подготовка и сдача экзамена.

В дисциплине можно выделить две области:

- базовые знания, относительно стабильные, составляющие ядро дисциплины;
- технологические знания, связанные с освоением конкретных программных систем компьютерной графики.

Базовые знания включают в себя системный подход к изучению теоретического материала, знание терминологии и современных особенностей и средств теории кодирования.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Компьютерный класс: 15 Моноблоков/HPP-B0G08ES#ACB| HP 8200E AiO i52400S 500G 4/0G 28PC, Проектор 3-chip DLP, 10 600 ANSI-лм, WUXGA 1 920x1 200 (16:10) PT-DZ110XE Panasonic; экран 316x500 см, 16:10 с эл. приводом; крепление настенно-потолочное Elpro Large Electrol Projecta; профессиональная ЖК-панель 47", 500 Кд/м2, Full HD M4716CCBA LG; подсистема видеоисточников документ-камера CP355AF Avervision; подсистема видеокоммутации; подсистема аудиокоммутации и звукоусиления; подсистема интерактивного управления; беспроводные ЛВС обеспечены системой на базе точек доступа. (Корпус 20, ауд. D 734, 734а, 546, 546а)

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Компьютерные классы ДВФУ (кампус на о. Русском, Аякс 10, корпус D, ауд. 734, 734а	15 Моноблоков/HPP-B0G08ES#ACB HP 8200E AiO i52400S 500G 4/0G 28PC	Системное и прикладное обеспечение ПЭВМ Windows Edu Per Device 10 Education Microsoft 365 Apps for enterprise EDU
Лекционная аудитория D546, D546а	Проектор 3-chip DLP, 10 600 ANSI-лм, WUXGA 1 920x1 200 (16:10) PT-DZ110XE Panasonic; экран 316x500 см, 16:10 с эл. приводом; крепление настенно-потолочное Elpro Large Electrol Projecta; профессиональная ЖК-панель 47", 500 Кд/м2, Full HD M4716CCBA LG; подсистема видеоисточников документ-камера CP355AF Avervision; подсистема видеокоммутации; подсистема аудиокоммутации и звукоусиления; подсистема интерактивного управления; беспроводные ЛВС обеспечены системой на базе точек доступа	Системное и прикладное обеспечение ПЭВМ Windows Edu Per Device 10 Education Microsoft 365 Apps for enterprise EDU

VIII. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Для дисциплины «Основы теории кодирования» используются следующие оценочные средства:

Устный опрос:

1. Конспект (ПР-7)
2. Собеседование (УО-1)

Письменные работы:

1. Лабораторная работа (ПР-6)
2. Контрольная работа (ПР-2)

Устный опрос

Устный опрос позволяет оценить знания и кругозор студента, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки.

Обучающая функция состоит в выявлении деталей, которые по каким-то причинам оказались недостаточно осмысленными в ходе учебных занятий и при подготовке к зачёту.

Собеседование (УО-1) – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Письменные работы

Письменный ответ приучает к точности, лаконичности, связности изложения мысли. Письменная проверка используется во всех видах контроля и осуществляется как в аудиторной, так и во внеаудиторной работе.

Лабораторная работа (ПР-6) – средство для закрепления и практического освоения материала по определенному разделу.

Контрольная работа (ПР-2) – средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Текущая аттестация студентов. Текущая аттестация студентов проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация проводится в форме собеседования (устного опроса) для проверки теоретических знаний, а также в форме защиты индивидуального задания, выполняемого в рамках самостоятельной работы параллельно с лабораторными и практическими работами и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

– степень усвоения теоретических знаний – оценивается в форме собеседования и контрольных работ;

– уровень овладения практическими умениями и навыками – оценивается в форме защиты индивидуального задания, выполняемого в рамках лабораторных.

Промежуточная аттестация студентов по дисциплине «Основы теории кодирования» проводится в соответствии с локальными нормативными актами ДВФУ в виде зачета в устной форме.

Вопросы к экзамену

1. Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Поточковые и блочные шифры.
2. Рандомизация проверки простоты (WITNESS). Числа Карлмайкла}
3. Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Поточковые и блочные шифры.
4. Протокол взаимной аутентификации. Схема обмена ключами Диффи-Хеллмана.
5. Модулярные шифры. Шифры Виженера. Автоматический и бегущий выбор ключа.
6. Теорема о корнях $x^2=1 \pmod p$ для нечетного простого p .
7. Шифры Вернама, Плейфейера, Хилла. Шифр одноразового блокнота. Абсолютно криптостойкие шифры.
8. Греко-китайская теорема об остатках и ее применения.
9. Шифр Файстеля. Структура шифра. Алгоритм дешифрования.
10. Малая теорема Ферма. Теорема Эйлера.
11. DES: алгоритмы шифрования и дешифрования. Надежность.
12. Криптоанализ. Диффузия и конфузия.
13. Возведение в степень с использованием метода последовательного возведения в квадрат.
14. Тройной DES.

15. Группы, кольца, области целостности, поля.
16. Двойной DES.
17. Криптосистемы, базирующиеся на задаче о рюкзаке.
18. Режимы работы DES. Сцепление блоков.
19. Обмен ключами по алгоритму ВВ84 (квантовая криптография).
20. Простые числа. Основная теорема арифметики. Теорема Евклида о существовании бесконечного множества простых чисел. Теорема о промежутках между простыми числами.
21. RSA: основные элементы криптосистемы. Шифрование и дешифрование.

Критерии оценивания на экзамене

Оценка	Требования к сформированным компетенциям
«отлично»	выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«хорошо»	выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«удовлетворительно»	выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
«неудовлетворительно»	выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Критерии оценки лабораторных работ

Оценка	Требования к сформированным компетенциям
«отлично»	Представлено оптимальное решение. Все тесты завершены успешно.
«хорошо»	Более 50% тестов завершены успешно. Выбран не оптимальный метод или отличный от указанного в задании.
«удовлетворительно»	Задание решено частично. Менее 50% тестов завершены успешно. Выбран не оптимальный метод или отличный от указанного в задании.
«неудовлетворительно»	Задание не решено. Нет успешного завершения ни для одного теста.