МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Согласовано
Школа естественных наук
Руководитель ОП
_____ _
(подпись) (С.Г. Должиков)
«__18___»__июня_____2015___г.

«УТВЕРЖДАЮ»
Заведующий кафедрой компьютерных систем
_____
(подпись) (Е.Л. Кулешов)
«__18___»__июня_____2015____г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (РПУД)
Основы криптографии
Направление подготовки:
09.03.02 Информационные системы и технологии
профиль Информационные системы и технологии в связи

Форма подготовки: очная

Школа естественных наук
Кафедра
Курс 3 семестр 5
лекции __36_ (час.)
лабораторные работы____0___час.
практические занятия___36____час.
в том числе с использованием МАО лекц. 0 / пр.18 час.
всего часов аудиторной нагрузки____72____ (час.)
в том числе с использованием МАО 36 час.
самостоятельная работа ____72_____ (час.)
в том числе на подготовку к экзамену _____ час.
Курсовая работа / курсовой проект – не предусмотрено
Контрольные работы __семестры
зачет 4 семестр
экзамен __ семестр

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии (уровень бакалавриата) утвержденного приказом Минобрнауки №219 от 12.03.2015г.

Рабочая программа обсуждена на заседании кафедры компьютерных систем, протокол № 14 от «18» июня 2015 г.

Заведующий кафедрой Кулешов Е.Л.
Составитель (ли): доцент кафедры алгебры, геометрии и анализа Чеканов С.Г., к.ф.-м.н.

Оборотная сторона титульного листа РПУД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 200 г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 200 г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

АННОТАЦИЯ

Криптография – это наука о математических методах защиты информации. До середины двадцатого века криптографические методы использовались, в основном, для защиты дипломатической почты, военных и государственных секретов. С середины двадцатого века, с бурным развитием информационных технологий потребность в криптографических методах возросла многократно. В настоящее время криптографические дисциплины включены в учебные планы всех направлений, связанных с информационными технологиями.

Очевидно, что технологические изменения потребуют новых методов и концепций, которые будут обеспечивать необходимые функции информационной безопасности.

Цель преподавания дисциплины: - знакомство студентов с современными понятиями и методами криптографии, основными криптографическими примитивами и протоколами.

Задачи преподавания дисциплины:

1. изучить классические шифры;
2. ознакомиться с современной классификацией криптографических примитивов;
3. изучить модели возможных атак на криптосистемы и методы оценки их стойкости;
4. применение полученных знаний для построения моделей криптосистем.

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции.

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОПК-6 способностью выбирать и оценивать способ реализации информационных	Знает	задачи и методы проектирования и разработки информационной системы предприятия и организации
	Умеет	адаптировать современные ИКТ к задачам прикладных ИС к проектированию и разработке информационной системы предприятия и

систем и устройств (программно-, аппаратно- или программно-аппаратно-) для решения поставленной задачи		организации
	Владеет	инструментальными средствами проектирования информационных процессов и систем
ПК-19 способностью к организации работы малых коллективов исполнителей	Знает	принципы работы малых коллективов исполнителей
	Умеет	организовать работу малых коллективов исполнителей
	Владеет	способностью к организации работы малых коллективов исполнителей
ПК-27 способностью формировать новые конкурентоспособные идеи и реализовывать их в проектах	Знает	новые идеи и проекты в области информационных технологий
	Умеет	формировать новые конкурентоспособные идеи и реализовывать их в проектах
	Владеет	способностью формировать новые конкурентоспособные идеи и реализовывать их в проектах

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы криптографии» применяются следующие методы активного/ интерактивного обучения: групповая консультация.

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

5 семестр (36 час.)

Тема 1. (2 час.) **«Классификация шифров. Математическая модель шифра замены».** Основные функции информационной безопасности. Модели шифров на основе алгебраических систем. Шифр простой замены.

Тема 2. (2 час.) **«Криптоанализ шифров простой замены».** Частотные характеристики текстов. Методы изменения характеристик текстов.

Тема 3. (4 час.) **«Шифр Виженера».** Многоалфавитные шифры. Индексы совпадений. Криптоанализ шифра Виженера.

Тема 4. (2 час.) **«Стойкость шифров. Энтропия и избыточность языка».** Статистические характеристики текстов. Энтропия языка и способы ее вычисления. Условная энтропия и совершенные шифры по Шеннону.

Тема 5. (2 час.) **«Имитостойкость шифров».** Активные атаки на шифры. Оценка стойкости шифров по отношению к активным атакам. Шифры не распространяющие искажений.

Тема 6. (2 час.) **«Блочные системы шифрования»**. Принципы построения блочных шифров. Методы анализа алгоритмов блочного шифрования.

Тема 7. (4 час.) **«Стандарты блочных шифров».** Американский стандарт блочного шифрования DES. Стандарт шифрования ГОСТ 28147-89.

Тема 8. (4 час.) **«Поточные системы шифрования»**.

Синхронизация поточных шифрсистем. Шифрсистема A5. Генераторы ключевых последовательностей. Линейные рекуррентные последовательности.

Тема 9. (2 час.) **«Асимметричные шифры. Шифр RSA».** Проблема факторизации на множестве целых чисел. Кодировка текстов элементами кольца вычетов. Алгоритмы шифрования и дешифрования.

Тема 10. (4 часов) **«Криптографические хеш функции».**

Характеристические свойства хеш функций. Область применения хеш-функций. Построение хеш функций на основе известных шифров.

Тема 11. (4 час.) **«Криптографические протоколы»**. Протоколы аутентификации и распределения ключей. Алгоритм Диффи-Хелмана. Оценка стойкости протоколов.

Тема 12. (2 час.) **«Цифровая подпись».** Схемы цифровой подписи на основе асимметричного шифра. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля.

Тема 13. (2 час.) **«Оценка стойкости криптографических протоколов с помощью неклассических логик».** Формализация понятия стойкого протокола в рамках логического исчисления. Построение алгоритмов проверки протоколов на соответствие заявленным свойствам информационной безопасности.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Трудоемкость практической части курса 36 час.

5 семестр (36 час.)

Занятие 1. Математические модели шифров замены (2 час.)

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Кодировка исходного алфавита элементами кольца вычетов. Представление алгоритмов шифрования элементами аффинной группы соответствующего модуля. Группа подстановок, как как множество ключей перестановочного шифра.

Занятие 2. Криптоанализ шифра простой замены (2 час.).

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Построение математической модели шифра простой замены. Решение задач криптоанализа с использованием частотного метода. Оценка вычислительной стойкости алгоритмов.

Занятие 4. Индексы совпадений (2 час.).

Занятие проводится **с использованием метода активного обучения «групповая консультация».**

Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация

проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Вычисление индексов совпадения для шифртекстов и определение связи с естественными языками. Написание соответствующих программ.

Занятие 3. Криптоанализ шифра Виженера. (2 час.)

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она

позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Определение длины ключа для шифра Виженера. Вычисление возможных сдвигов элементов ключа относительно друг друга. Восстановление открытого текста.

Занятие 4. Энтропия языка (2 час.).

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Энтропия случайной величины. Информационная составляющая энтропии языка. Избыточность языка. Условная энтропия.

Занятие 5. Имитостойкость шифров (2 час.).

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Оценка имитостойкости шифров в рамках известных математических моделей. Решение задач о распространении ошибок шифрами. Решение проблемы синхронизации.

Занятие 6. Блочные системы шифрования (2 час.).

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью

оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Построение простейших блочных шифров. Особенности криптоанализа блочных шифров. Выявление сильных и слабых сторон блочных шифров.

Занятие 7. Стандарт шифрования DES (2 час.)

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим

интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Компоненты алгоритма шифрования. Генерация раундовых ключей в DES. Построение шифртекста по открытому тексту и ключу. Таблицы S-блоков.

Занятие 8. Стандарт шифрования ГОСТ 28147-89. (2 час.).

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Алгоритм шифрования и генерация раундовых ключей. Характеристики блоков. Шифрование конкретных текстов.

Занятие 9. Линейные рекуррентные последовательности (2 час.)

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой

своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Линейные рекуррентные последовательности. Характеристический полином ЛРП. Оценка периода ЛРП. Построение генераторов ключевых последовательностей. Атаки на генераторы.

Занятие 10. Генератор ключевой последовательности A5 (2 часа)

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые

вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Характеристические полиномы генератора. Функция изменения состояния генератора и выходная функция. Построение ключевой последовательности.

Занятие 11. Асимметричные шифры (2 час.)

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс

обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Задача факторизации целых чисел. Мультипликативная группа кольца вычетов. Представление текстов естественного языка элементами мультипликативной группы. Решение задач шифрования и дешифрования в RSA.

Занятие 11. Хеш функции (2 час.)

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Характеристические свойства хеш функций. Логическая независимость различных свойств хеш функций. Построение примеров на основе симметричных шифров.

Занятие 12. Криптоанализ хеш функций (2 час.)

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Примеры хеш функций на основе асимметричных шифров. Оценка вычислительной сложности построения прообраза и коллизии.

Занятие 13. Криптографические протоколы (2 час.)

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной

контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Функции безопасности криптографических протоколов. Протоколы аутентификации. Алгоритм Диффи-Хелмана. Построение протоколов с заданными свойствами.

Занятие 14. Оценка стойкости протоколов (2 часа)

Занятие проводится **с использованием метода активного обучения «групповая консультация».** Групповые консультации представляют собой своеобразную форму проведения практических занятий, основным содержанием которых является разъяснение отдельных, часто наиболее сложных или практически значимых вопросов изучаемой программы. После всех практических занятий студенты получают задачи для самостоятельной внеаудиторной работы. С каждым практическим занятием повышается сложность предлагаемых задач. Групповая консультация проводятся с целью оказания помощи в самостоятельной работе, в подготовке к рубежной контрольной работе. Студенты сами предлагает для решения те задачи, которые вызвали какие-то затруднения или непонимание. К доске выходят студенты, готовые разъяснить возникшие вопросы. Преподаватель только контролирует ход решения задач, комментирует в случае необходимости какие-то ситуации и обобщает рассмотренный материал. Преимущество практики-консультации перед другими формами проведения практического занятия в том, что она позволяет в большей степени приблизить содержание занятия к практическим интересам обучаемых, в какой-то степени индивидуализировать процесс

обучения с учетом уровня понимания и восприятия материала каждым обучаемым.

Построение простейших протоколов и оценка их безопасности. Обоснование необходимости раундов протокола.

Занятие 15. Цифровые подписи (2 часа)

Концепция цифровой подписи и возможные криптографические примитивы, необходимые для ее создания. Цифровая подпись Фиата-Шамира.

Занятие 16. Протоколы и неклассические логики (2 часа)

Неклассические логические исчисления. Модальные и темпоральные логики. BAN – логика. Анализ протоколов аутентификации и генерации ключей в рамках BAN – логики.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Основы криптографии» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Классические шифры	ОПК-6 ПК-19 ПК-27	знает	еоретические диктанты	зачет, вопросы 1-21
			умеет	Решение задач по изучаемой теме на практических занятиях Контрольная работа (ПР-2)	зачет, вопросы 1-21

			владеет	Индивидуальные домашние здания	зачет, вопросы 1-21
2	Модели шифров	ОПК6 ПК-19 ПК-27	знает	Теоретические диктанты	зачет, вопросы 1-21
			умеет	Решение задач по изучаемой теме на практических занятиях Контрольная работа (ПР-2)	зачет, вопросы 1-21
			владеет	Индивидуальные домашние здания	зачет, вопросы 1-21
3	Энтропия языка	ОПК6 ПК-19 ПК-27	знает	Летучий устный или письменный опрос студентов во время лекции по изучаемому материалу	зачет, вопросы 1-21
			умеет	Решение задач по изучаемой теме на практических занятиях Контрольная работа (ПР-2)	зачет, вопросы 1-21
			владеет	Индивидуальные домашние здания	зачет, вопросы 1-21
4	Блочные шифры	ОПК6 ПК-19 ПК-27	знает	Теоретические диктанты	зачет, вопросы 1-21
			умеет	Решение задач по изучаемой теме на практических занятиях Контрольная работа (ПР-2)	зачет, вопросы 1-21
			владеет	Индивидуальные домашние здания	зачет, вопросы 1-21
5	Поточные шифры	ОПК6 ПК-19 ПК-27	знает	Летучий устный или письменный опрос студентов во время лекции по изучаемому материалу	зачет, вопросы 1-21
			умеет	Решение задач по изучаемой теме на практических занятиях Контрольная работа (ПР-2)	зачет, вопросы 1-21
			владеет	Индивидуальные домашние здания	зачет, вопросы 1-21
6	Криптографические протоколы	ОПК6 ПК-19 ПК-27	знает	Теоретические диктанты	зачет, вопросы 1-21
			умеет	Решение задач по изучаемой теме на практических занятиях	зачет, вопросы 1-21

				Контрольная работа (ПР-2)	
			владеет	Индивидуальные домашние здания	зачет, вопросы 1-21

Типовые контрольные задания и вопросы к зачету представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

№	название	Ссылка в ЭК НБ ДВФУ	Внешняя ссылка
1	Криптографические методы защиты информации: учебное пособие для вузов / Б. Я. Рябко, А. Н. Фионов. Москва: Горячая линия - Телеком, 2013. – 229 с.	https://lib.dvfu.ru:8443/lib/item?id=chamo:692852&theme=FEFU	
2	Практикум по криптосистемам с открытым ключом: [учебное пособие для инженерно-технических вузов] / Н. А. Молдовян Санкт-Петербург : БХВ-Петербург, 2014. – 298 с.	https://lib.dvfu.ru:8443/lib/item?id=chamo:845682&theme=FEFU	
3	Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А. И. Астайкин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко. — Электрон. текстовые данные. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 224 c. — 978-5-9515-0305-3.	https://lib.dvfu.ru:8443/lib/item?id=IPRbooks:IPRbooks-60959&theme=FEFU	http://www.iprbookshop.ru/60959.html
4	Калмыков, И. А. Криптографические методы защиты информации [Электронный ресурс] : лабораторный практикум / И. А.	https://lib.dvfu.ru:8443/lib/item?id=IPRbooks:IPRbooks-63099&theme=FEFU	http://www.iprbookshop.ru/63099.html

	Калмыков, Д. О. Науменко, Т. А. Гиш. — Электрон. текстовые данные. — Ставрополь : Северо-Кавказский федеральный университет, 2015. — 109 c. — 2227-8397.		

Дополнительная литература

№	название	Ссылка в ЭК НБ ДВФУ	Внешняя ссылка
1	Рябко, Борис Яковлевич. Криптография и стенография в информационных технологиях / Б. Я. Рябко, А. Н. Фионов, Ю. И. Шокин;; Российская академия наук, Сибирское отделение, Новосибирск : Наука, 2015.239 с.	http://lib.dvfu.ru:8080/lib/item?id=chamo:801781&theme=FEFU	

Интернет-ресурсы

1. 1. Коржик В.И., Яковлев В.А. Основы криптографии, учебное пособие: учебное пособие. Изд-во: ИЦ Интермедия, 2016, 296 с. https://e.lanbook.com/book/90264#book_name
2. Журнал Открытые системы: http://www.osp.ru/os/#/home
3. Международный компьютерный журнал: http://www.computerworld.ru/
4. Журнал iXBT: http://mag.ixbt.com/

VI. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

На изучение дисциплины отводится 72 часа аудиторных занятий. На лекциях преподаватель объясняет теоретический материал. Вводит основные понятия, определения, свойства. Формулирует и доказывает теоремы. Приводит примеры. Необходимо поддерживать непрерывный контакт с аудиторией, отвечать на возникающие у студентов вопросы. На практических занятиях преподаватель разбирает примеры по пройденной теме. Во второй

части занятия студентам предлагается работать самостоятельно, выполняя задания по теме. Преподаватель контролирует работу студентов, отвечает на возникающие вопросы, подсказывает ход и метод решения. Если знаний полученных в аудитории оказалось недостаточно, студент может самостоятельно повторно прочитать лекцию. После выполнения задания, студент отправляет его на проверку преподавателю. Работа должна быть отослана в формате PDF одним документом. По данному курсу разработаны методические указания.

По данному курсу разработаны методические указания:

1. Чеканов С.Г., Степанова А.А. Основы теории конечных групп. Учебное пособие.
2. Чеканов С.Г., Степанова А.А. Конечные поля. Учебное пособие.

VII МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения исследований, связанных с выполнением задания по практике, а также для организации самостоятельной работы студентам доступно следующее лабораторное оборудование и специализированные кабинеты, соответствующие действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-производственных работ:

Наименование оборудованных помещений и помещений для самостоятельной работы	Перечень основного оборудования
Владивосток, о. Русский, п. Аякс д.10, корпус L, ауд. L 502 учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и	учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации

промежуточной аттестации	
Владивосток, о. Русский, п. Аякс д.10, корпус L, ауд. L 558 учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Парты и стулья
Читальные залы Научной библиотеки ДВФУ с открытым доступом к фонду (корпус А - уровень 10) Учебная аудитория для проведения самостоятельной работы	Моноблок HP ProOne 400 All-in-One 19,5 (1600x900), Core i3-4150T, 4GB DDR3-1600 (1x4GB), 1TB HDD 7200 SATA, DVD+/-RW,GigEth,Wi-Fi,BT,usb kbd/mse,Win7Pro (64-bit)+Win8.1Pro(64-bit),1-1-1 Wty Скорость доступа в Интернет 500 Мбит/сек. Рабочие места для людей с ограниченными возможностями здоровья оснащены дисплеями и принтерами Брайля; оборудованы: портативными устройствами для чтения плоскопечатных текстов, сканирующими и читающими машинами видеоувелечителем с возможностью регуляции цветовых спектров; увеличивающими электронными лупами и ультразвуковыми маркировщиками

В целях обеспечения специальных условий обучения инвалидов и лиц с ограниченными возможностями здоровья в ДВФУ все здания оборудованы пандусами, лифтами, подъемниками, специализированными местами, оснащенными туалетными комнатами, табличками информационно-навигационной поддержки.

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Основы криптографии»

Направление подготовки: 09.03.02 информационные системы и технологии,
профиль Информационные системы и технологии в связи

Форма подготовки очная

Владивосток
2015

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1.	1 – 3 неделя обучения	индивидуальное домашнее задание	12 час	проверка выполнения ИДЗ
2.	4 – 6 неделя обучения	индивидуальное домашнее задание	12 час	проверка выполнения ИДЗ
3.	7 – 8 неделя обучения	индивидуальное домашнее задание	12 час	проверка выполнения ИДЗ
4.	9 – 11 неделя обучения	индивидуальное домашнее задание	12 час	проверка выполнения ИДЗ
4.	12 – 14 неделя обучения	индивидуальное домашнее задание	12 час	проверка выполнения ИДЗ
5.	15 – 16 неделя обучения	индивидуальное домашнее задание	12 час	проверка выполнения ИДЗ
6.	17 – 18 неделя обучения	индивидуальное домашнее задание	12 час	проверка выполнения ИДЗ
			72 часа	

Материалы для самостоятельной работы студентов подготовлены в виде индивидуальных домашних заданий по каждой теме (образцы типовых ИДЗ представлены в разделе «Материалы для самостоятельной работы студентов»). Работа должна быть отправлена преподавателю. Оформление в формате PDF. Критерии оценки: студент получает максимальный балл, если работа выполнена без ошибок и оформлена в соответствии с требованиями преподавателя.

Рекомендации по работе с литературой

Для более эффективного освоения и усвоения материала рекомендуется ознакомиться с теоретическим материалом по той или иной теме до

проведения лабораторного занятия. Всю учебную литературу желательно изучать «под конспект».

Цель написания конспекта по дисциплине – сформировать навыки по поиску, отбору, анализу и формулированию учебного материала.

Работу с теоретическим материалом по теме можно проводить по следующей схеме:

- название темы;

- цели и задачи изучения темы;

- основные вопросы темы;

- характеристика основных понятий и определений, необходимых для усвоения данной темы;

- краткие выводы, ориентирующие на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить.

При работе над конспектом обязательно выявляются и отмечаются трудные для самостоятельного изучения вопросы, с которыми уместно обратиться к преподавателю при посещении консультаций, либо в индивидуальном порядке.

Приложение 2

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»
(ДВФУ)
ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Основы криптографии»

Направление подготовки: 09.03.03 информационные системы и технологии,
профиль Информационные системы и технологии в связи

Форма подготовки очная

Владивосток
2015

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-6 - способностью выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно-) для решения поставленной задачи	Знает	задачи и методы проектирования и разработки информационной системы предприятия и организации
	Умеет	адаптировать современные ИКТ к задачам прикладных ИС к проектированию и разработке информационной системы предприятия и организации
	Владеет	инструментальными средствами проектирования информационных процессов и систем
ПК-19 способностью к организации работы малых коллективов исполнителей	Знает	принципы работы малых коллективов исполнителей
	Умеет	организовать работу малых коллективов исполнителей
	Владеет	способностью к организации работы малых коллективов исполнителей
ПК-27 способностью формировать новые конкурентоспособные идеи и реализовывать их в проектах	Знает	новые идеи и проекты в области информационных технологий
	Умеет	формировать новые конкурентоспособные идеи и реализовывать их в проектах
	Владеет	способностью формировать новые конкурентоспособные идеи и реализовывать их в проектах

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Классические шифры	ОПК6 ПК-19 ПК-27	Знает	- Устный или письменный опрос студентов во время лекции по изучаемому материалу; - Теоретические диктанты;	зачет, вопросы 1-21

			Умеет Владеет	- Решение задач по изучаемой теме на практических занятиях; - Индивидуальные домашние здания; - Контрольная работа (ПР-2)	
2	Модели шифров	ОПК6 ПК-19 ПК-27	Знает	- Устный или письменный опрос студентов во время лекции по изучаемому материалу; - Теоретические диктанты;	зачет, вопросы 1-21
			Умеет Владеет	- Решение задач по изучаемой теме на практических занятиях; - Индивидуальные домашние здания; - Контрольная работа (ПР-2)	
3	Энтропия языка	ОПК6 ПК-19 ПК-27	Знает	- Устный или письменный опрос студентов во время лекции по изучаемому материалу; - Теоретические диктанты;	зачет, вопросы 1-21
			Умеет Владеет	- Решение задач по изучаемой теме на практических занятиях; - Индивидуальные домашние здания;	

				- Контрольная работа (ПР-2)	
4	Блочные шифры	ОПК6 ПК-19 ПК-27	Знает	- Устный или письменный опрос студентов во время лекции по изучаемому материалу; - Теоретические диктанты;	зачет, вопросы 1-21
			Умеет Владеет	- Решение задач по изучаемой теме на практических занятиях; - Индивидуальные домашние здания; - Контрольная работа (ПР-2)	
5	Поточные шифры	ОПК6 ПК-19 ПК-27	Знает	- Устный или письменный опрос студентов во время лекции по изучаемому материалу; - Теоретические диктанты;	зачет, вопросы 1-21
			Умеет Владеет	- Решение задач по изучаемой теме на практических занятиях; - Индивидуальные домашние здания;	
6	Криптографические протоколы	ОПК6 ПК-19 ПК-27	Знает	- Устный или письменный опрос студентов во время лекции по изучаемому материалу; - Теоретические диктанты;	зачет, вопросы 1-21
			Умеет	- Решение задач	

			Владеет	по изучаемой теме на практических занятиях; - Индивидуальные домашние здания; - Контрольная работа (ПР-2)	

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
ОПК-6 – способность выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно) для решения поставленной задачи	знает (пороговый уровень)	методы анализа, выбора и обоснования методологии и технологии проектирования базовых и прикладных информационных технологий; содержание проектных работ в создании и эксплуатации базовых и прикладных информационных технологий	воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты	способность показать базовые знания и основные умения в использовании: - базовых стандартов графического описания архитектур ИС; - диаграмм и схем в проектной документации
	умеет (продвинутый)	разрабатывать проекты и выполнять проектные работы по созданию, внедрению и эксплуатации базовых и прикладных информационных технологий	решать типичные задачи на основе воспроизведения стандартных алгоритмов решения	способность применить знания и практические умения при разработке архитектурных схем для представления ИС в проектной документации
	владеет (высокий)	навыками разработки ведения	решать усложненные задачи в	способность применить фактическое и

		проектных работ по созданию, внедрению и эксплуатации базовых и прикладных информационных технологий	нетипичных ситуациях на основе приобретенных знаний, умений и навыков	теоретическое знание, практические умения по разработке архитектурных схем для представления ИС в проектной документации
ПК-19 способностью к организации работы малых коллективов исполнителей	знает (пороговый уровень)	принципы работы малых коллективов исполнителей	знание способов организации работы малых коллективов исполнителей	способен рассказать способы организации работы малых коллективов исполнителей и методы работы в коллективе и способы организации работы малых коллективов исполнителей
	умеет (продвинутый)	организовать работу малых коллективов исполнителей	умение эффективно работать в коллективе	способность эффективно работать в коллективе и решать поставленные задачи
	владеет (высокий)	способностью к организации работы малых коллективов исполнителей	владение навыками организации работы малых коллективов исполнителей	способность организовывать работу малых коллективов исполнителей на предприятиях
ПК-27 способностью формировать новые конкурентоспособные идеи и реализовывать их в проектах	знает (пороговый уровень)	новые идеи и проекты в области информационных технологий	знание основных принципов создания и оформления проектов, в том числе связанных с численным моделированием	способность описать способы формирования новых конкурентоспособных идей и основные принципы создания и оформления проектов, в том числе связанных с численным моделированием
	умеет (продвинуты	формировать новые	проводить оценку	способность самостоятельно

	й)	конкурентоспособные идеи и реализовывать их в проектах	конкурентоспособности идей и предложений	выдвигать новые идеи, проводить оценку конкурентоспособности идей и предложений.
	владеет (высокий)	способностью формировать новые конкурентоспособные идеи и реализовывать их в проектах	владение способностью анализировать имеющуюся научно-техническую информацию; навыками вербализации, содержательного описания наблюдений, интерпретации смысла новых явлений в физических системах	способен на высоком уровне пользоваться навыками вербализации, содержательного описания наблюдений, интерпретации смысла новых явлений в физических системах

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 выполненных практических заданий.

Объектами оценивания выступают:

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

– уровень овладения практическими умениями и навыками – оценивается в форме защиты задания.

Критерии оценки устного ответа

– **100-85 баллов** - если ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой

раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

– **85-76 баллов** - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

– **75-61 балл** - оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

– **60-50** баллов - ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области

Критерии оценки практических заданий

100-86 баллов выставляется, если содержание и составляющие части соответствуют выданному заданию. Продемонстрировано владение навыками выбора необходимых формул и построений выводов.

85-76 - баллов выставляется, если при выполнении задания допущено не более одной ошибки.

75-61 балл выставляется, если при выполнении задания допущено не более двух ошибок.

60-50 баллов - если структура и содержание задания не соответствуют требуемым

Шкала оценивания

Менее 60 баллов	не зачтено	неудовлетворительно
От 61 до 75 баллов	зачтено	удовлетворительно
От 76 до 85 баллов	зачтено	хорошо
От 86 до 100 балов	зачтено	отлично

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

По дисциплине предусмотрен экзамен.

Оценочные средства для промежуточной аттестации

Вопросы к зачету

1. Шифр простой замены
2. Перестановочные шифры
3. Аффинные шифры над конечными полями
4. Мультипликативная группа кольца вычетов
5. Алгебраическая модель шифра

6. Вероятностная модель шифра

7. Шифр Виженера

8. Энтропия и избыточность языка

9. Теоретическая и практическая стойкость шифров

10. Имитостойкость шифров

11. Блочные шифры

12. Линейные рекуррентные последовательности

13. Поточные шифры и генераторы ключевых последовательностей

14. Проблема факторизации в целых числах и шифр RSA.

15. Шифр Эль Гамаля.

16. Хеш функции.

17. Протоколы аутентификации.

18. Цифровые подписи

19. Алгоритм DES

20. Генератор ключевой последовательности A5

21. Анализ стойкости протоколов в неклассических логиках

Оценочные средства для текущей аттестации

Примеры вариантов контрольных работ

Контрольная работа №1 по теме «Проблема факторизации и шифр RSA»

1 вариант

1. Найдите каноническое представление числа:
   а) 92772757 ; б) 40! .

2. Найдите наибольший общий делитель систем чисел:
   а) 105369 и 4991 (по алгоритму Евклида);

б) 216270, 192329 и 178178 (через каноническое представление).

3. Найдите наименьшее общее кратное систем чисел:
   а) 720 и 1512 (по формуле);

б) 96, 64 и 20 (через каноническое представление чисел).

4. Найдите число делителей, сумму делителей и значение функции Эйлера для числа n = 343343.
5. Дано: $\varphi(n) = 3600$, $n = 3^{\alpha} \cdot 5^{\beta} \cdot 11^{\gamma}$. Найдите n.
6. Найдите две последние цифры числа 17^{61}.
7. Решите сравнение:
   а) $12x \equiv 4 \pmod 5$, б) $49x \equiv 14 \pmod{77}$.
8. Решите систему сравнений: $\begin{cases} x \equiv 7 \pmod{17}; \\ x \equiv 3 \pmod{14}. \end{cases}$
9. Докажите, что если $(a,b) = 1$, то наибольший общий делитель чисел $a+b$ и a^2+b^2 равен либо 1, либо 2.
10. Докажите, что $53^{53} - 33^{33}$ делится на 10.

2 вариант

1. Найдите каноническое представление числа:
   а) 97363981 ; б) 19! .
2. Найдите наибольший общий делитель систем чисел:
   а) 62510 и 23731 (по алгоритму Евклида);

б) 454532, 174820 и 82287 (через каноническое представление).

3. Найдите наименьшее общее кратное систем чисел:
   а) 180 и 504 (по формуле);

   б) 28, 22 и 44 (через каноническое представление чисел).
4. Найдите число делителей, сумму делителей и значение функции Эйлера для числа n = 225225.
5. Решите уравнение: $\varphi(5^x) = 2500$.
6. Найдите две последние цифры числа 7^{114}.
7. Решите сравнение:
   а) $13x \equiv 5 \pmod{21}$, б) $88x \equiv 14 \pmod{26}$.
8. Решите систему сравнений: $\begin{cases} x \equiv 4 \pmod{15}; \\ x \equiv 13 \pmod{21}. \end{cases}$
9. Докажите, что если $(a,b) = 1$, то наибольший общий делитель чисел $11a+2b$ и $18a+5b$ равен либо 1, либо 19.
10. Найдите наибольшее трехзначное число, при делении которого на 4 получается в остатке 3, при делении на 5 в остатке 4, при делении на 6 в остатке 5.

3 вариант

1. Найдите каноническое представление числа:
   а) 29520491; б) 25! .
2. Найдите наибольший общий делитель систем чисел:
   а) 72181 и 7279 (по алгоритму Евклида);

б) 46330, 197750 и 95372 (через каноническое представление).

3. Найдите наименьшее общее кратное систем чисел:
   а) 270 и 405 (по формуле);

   б) 16, 40, 24 и 8 (через каноническое представление чисел).

4. Найдите число делителей, сумму делителей и значение функции Эйлера для числа n = 129600.
5. Дано: $\varphi(n) = 360$, $n = 3^{\alpha} \cdot 5^{\beta}$. Найдите n.
6. Найдите две последние цифры числа 11^{203}.
7. Решите сравнение:
   а) $24x \equiv 6 \pmod{25}$, б) $45x \equiv 105 \pmod{115}$.
8. Решите систему сравнений: $\begin{cases} x \equiv 7 \pmod{15}; \\ x \equiv 11 \pmod{25}. \end{cases}$
9. Докажите, что если $f(x)$ - многочлен с целыми коэффициентами, a и b - натуральные числа, причем $(a,b) = 1$, $f(a)$ делится на произведение ab, $f(b)$ делится на произведение ab, то $f(a+b)$ также делится на произведение ab.
10. Докажите, что если при $n > 2$ одно из чисел $2^n + 1$ и $2^n - 1$ - простое, то второе будет составным (при $n = 2$ оба числа простые).

4 вариант

1. Найдите каноническое представление числа:
   а) 71899443; б) 31! .
2. Найдите наибольший общий делитель систем чисел:
   а) 32219 и 19285 (по алгоритму Евклида);

б) 365010, 26220 и 230230 (через каноническое представление).

3. Найдите наименьшее общее кратное систем чисел:
   а) 666 и 555 (по формуле);

   б) 15, 35 и 25 (через каноническое представление чисел).

4. Найдите число делителей, сумму делителей и значение функции Эйлера для числа n = 96096.
5. Составьте таблицы сложения и умножения по модулю 14.
6. Найдите две последние цифры числа 7^{302}.
7. Решите сравнение:
   а) $53x \equiv 29 \pmod{105}$, б) $56x \equiv 16 \pmod{116}$.
8. Решите систему сравнений: $\begin{cases} x \equiv 3 \pmod{35}; \\ x \equiv 18 \pmod{55}; \\ x \equiv 24 \pmod{91}. \end{cases}$
9. Найдите 10 последовательных составных чисел.
10. Цифры трехзначного числа - последовательные натуральные числа. Найдите разность между данным числом и числом, записанным теми же цифрами, но в обратном порядке.

Примеры вариантов тестовых заданий с ответами

1 вариант

№	Вопрос	Ответ
1	**Что такое шифрование?** а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств в) удобная среда для вычисления конечного пользователя	а)
2	**Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:** а) 1 б) 2 в) 3	а)
3	**Выберите то, как связаны ключи друг с другом в системе с открытым ключом:** а) математически б) логически в) алгоритмически	а)

2 вариант

№	Вопрос	Ответ
1	**Количество используемых ключей в системах с открытым ключом:** а) 2 б) 3 в) 1	а)
2	**Выберите то, что относится к показателям криптостойкости:** а) количество всех возможных ключей б) среднее время, необходимое для криптоанализа в) количество символов в ключе	а) б)
3	**Самая простая разновидность подстановки:** а) простая замена б) перестановка в) простая перестановка	а)

Примеры индивидуальных домашних заданий

Тема: Метод резолюций в алгебре высказываний

Проверить истинность следующих соотношений (3-мя способами):

1. $A \models A \vee C$,
2. $A \to B, B \to C \models A \to C$,
3. $A \to B, \overline{B} \models \overline{A}$.

Тема: Логика предикатов

1. Пусть Φ, Ψ, X - атомарные формулы логики предикатов. Выписать все подформулы данной формулы и определить свободные и связанные переменные формулы:

$\neg((\exists x \forall y \Phi(x,y) \vee \exists x \exists y \Psi(x,y)) \wedge \exists x \exists y X(x,y))$

2. Записать формулу $\Phi(x,y,z)$, истинную в $\langle N;+,\cdot \rangle$ тогда и только тогда, когда:

z = НОК (x,y)

3. Записать формулу $\Phi(x)$, истинную в $\langle N;+,\cdot \rangle$ тогда и только тогда, когда:

x – простое число.

4. Пусть Φ, Ψ, X – атомарные формулы логики предикатов. Привести следующую формулу логики предикатов к пренексной нормальной форме

$$\neg((\exists x \forall y \Phi(x,y) \to \exists x \exists y \Psi(x,y)) \wedge \forall x \exists y \neg X(x,y))$$

Тема: Исчисление предикатов

Пусть Φ, Ψ, X, Θ - формулы исчисления предикатов. Построить вывод формулы исчисления предикатов из данного множества гипотез.

1. $\exists x \forall y \Phi(x,y) \vdash \exists z \Phi(z,z)$;
2. $\exists x(\Phi(x) \to \Psi(x)) \vdash \forall x \Phi(x) \to \exists y \Psi(y))$;
3. $\forall y(\Phi(x,y) \vee \Psi(x)) \vdash \exists x \exists z \Phi(z,x) \vee \exists x \Psi(x)$

Тема: Частично рекурсивные функции

Доказать, что следующие функции примитивно рекурсивны:

1. *min(x,y)*;
2. *rest(x,y)* – остаток от деления *x* на *y* (здесь *rest(x,0)=x*).

Доказать, что следующие функции частично рекурсивны:

$$f(x,y) = \begin{cases} \frac{x}{y}, \text{если } x \text{ делится на } y, \\ \text{не определена в остальных случаях;} \end{cases}$$

$$f(x,y) = \begin{cases} z, \text{если } z^y = x, \\ \text{не определена в остальных случаях;} \end{cases}$$