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

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

СОГЛАСОВАНО
Руководитель ОП

Р.И. Дремлюга

«17» июня .2019 г.

УТВЕРЖДАЮ
Директор Школы цифровой экономики

_____ И.Г. Мирин

«17» _____ 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ПРИКЛАДНАЯ КРИПТОГРАФИЯ»
направления 09.04.01 Информатика и вычислительная техника
Магистерская программа «Кибербезопасность»
Форма подготовки очная

курс 1 семестр 2
лекции 18 час.
практические занятия 36 час.
лабораторные работы 0 час.
всего часов аудиторной нагрузки 54 час.
самостоятельная работа 54 час.
контрольные работы программой не предусмотрены
курсовая работа/проект – не предусмотрено
зачет с оценкой 2 семестр
экзамен – не предусмотрено учебным планом

Рабочая программа составлена в соответствии составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки/специальности 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 918.

Рассмотрена и утверждена на заседании Дирекции Школы цифровой экономики «17» июня 2019 года (протокол № 124-01-07-05).

Составитель: ст.пр. Зотов С.С.

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании Дирекции Школы цифровой экономики:
Протокол от «_____» _____ 20___ г. № _____

Заместитель директора ШЦЭ
по учебной и воспитательной работе _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании Дирекции Школы цифровой экономики:
Протокол от «_____» _____ 20___ г. № _____

Заместитель директора ШЦЭ
по учебной и воспитательной работе _____ _____
(подпись) (И.О. Фамилия)

АННОТАЦИЯ
Б1.В.ДВ.01.08 ПРИКЛАДНАЯ КРИПТОГРАФИЯ

Рабочая программа дисциплины «Прикладная криптография» предназначена для студентов, обучающихся по направлению подготовки 09.04.01 Информатика и вычислительная техника (уровень магистратуры), профиль «Кибербезопасность».

Дисциплина «Прикладная криптография» входит в часть, формируемую участниками образовательных отношений, блока «Дисциплины (модули) Б1» (Б1.В.ДВ.01) учебного плана подготовки магистров, модуль элективных дисциплин

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы или 108 часов. Дисциплина реализуется на 1 курсе в 2 семестре.

Семестр	Аудиторные Занятия			Самостоятельная работа	Контроль	Форма контроля	Всего по дисциплине	
	Лекции	Лабораторные занятия	Практические занятия				Часы	з.е.
2 семестр	18	-	36	54	-	Зачет с оценкой	108	3

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

Задачи:

1. Изучение математических основ криптологии;
2. Выработка умений для анализа и реализации в виде программного обеспечения алгоритмов и протоколов, используемых при защите информации;
3. Формирование представлений о роли информационных технологий в жизни общества. Изучение методов тестирования безопасности информационной системы.

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.

Знания и практические навыки, полученные в результате освоения дисциплины «Прикладная криптография», используются студентами при разработке выпускных квалификационных работ.

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные и профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**
ОПК-2. Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.1 Знать: современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач ОПК-2.2 Уметь: обосновывать выбор современных информационно-коммуникационных и интеллектуальных технологий, разрабатывать оригинальные программные средства для решения профессиональных задач ОПК-2.3 Владеть: навыками разработки оригинальных программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий, для решения профессиональных задач
ОПК-7. Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий	ОПК-7.1 Знать: функциональные требования к прикладному программному обеспечению для решения актуальных задач предприятий отрасли, национальные стандарты обработки информации и автоматизированного проектирования ОПК-7.2 Уметь: приводить зарубежные комплексы обработки информации в соответствие с национальными стандартами, интегрировать с отраслевыми информационными системами ОПК-7.3 Владеть: навыками настройки интерфейса, разработки

	пользовательских шаблонов, подключения библиотек, добавления новых функций
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	ПК-2.1 Знает: модели безопасности компьютерных сетей; виды политик безопасности компьютерных систем и сетей; нормативно-правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации; организационные меры по защите информации ПК-2.2 Умеет: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем ПК-2.3 Владеет: навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; разработки руководящих документов по защите информации в организации

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекция 1. Блочные симметричные итеративные шифры (2 часа)

DES: шифрование и дешифрование. Лавинный эффект. Надежность. Криптоанализ. Режимы работы DES. Сцепление блоков. Шифрованная обратная связь Двойной и тройной DES. Другие симметрично-блочные шифры.

Лекция 2. Элементы теории сложности вычислений. (2 часа)

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

Лекция 3. Криптосистемы с открытым ключом (2 часа)

Группы, кольца, области целостности, поля. Классы вычетов по модулю. Малая теорема Ферма. Теорема Эйлера.

RSA: основные элементы криптосистемы. Шифрование и дешифрование.

Лекция 4. Аутентификация (2 часа)

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

Лекция 5. Современные проблемы (2 часа)

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

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (26 час.)

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

Занятие проводится с использованием метода активного обучения «групповая консультация

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». 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».

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

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

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

Занятие 4. Энтропия языка (2 час.).

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

Занятие 5. Имитостойкость шифров (2 час.).

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

Занятие 6. Блочные системы шифрования (2 час).

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

Занятие 7. Стандарт шифрования DES (1 час.)

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

Занятие 8. Стандарт шифрования ГОСТ 28147-89. (1 час.).

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

Занятие 9. Линейные рекуррентные последовательности (2 час.)

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

Занятие 10. Генератор ключевой последовательности А5 (2 часа)

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

Занятие 11. Асимметричные шифры (2 час.)

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.)

Характеристические свойства хеш функций. Логическая независимость различных свойств хеш функций. Построение примеров на основе симметричных шифров. Примеры хеш функций на основе асимметричных шифров. Оценка вычислительной сложности построения прообраза и коллизии.

Занятие 12. Криптографические протоколы (2 час.)

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

Занятие 13. Оценка стойкости протоколов (2 часа)

Построение простейших протоколов и оценка их безопасности. Обоснование необходимости раундов протокола. Неклассические логические исчисления. Модальные и темпоральные логики. BAN - логика. Анализ протоколов аутентификации и генерации ключей в рамках BAN - логики.

Занятие 14. Цифровые подписи (2 часа)

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

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Криптография» 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;
- требования к представлению и оформлению результатов самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии

характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1.Калмыков, И. А. Криптографические методы защиты информации [Электронный ресурс] : лабораторный практикум / И. А. Калмыков, Д. О. Науменко, Т. А. Гиш. — Электрон. текстовые данные. — Ставрополь : Северо-Кавказский федеральный университет, 2015. — 109 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63099.html

2. 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. — Режим доступа: https://lib.dvfu.ru:8443/lib/item?id=IPRbooks:IPRbooks-60959&theme=FEFU

3. Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс] : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Электрон. текстовые данные. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 95 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/17925.html

4. Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс] : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Электрон. текстовые данные. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 104 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/17926.html

Дополнительная литература

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. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации [Электронный ресурс] / сост. А. Э. Смирнов, Ю. А. Пономарёва. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 67 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61738.html

3. Рябко, Борис Яковлевич. Криптография и стенография в информационных технологиях / Б. Я. Рябко, А. Н. Фионов, Ю. И. Шокин; Российская академия наук, Сибирское Новосибирск : Наука, 2015.239 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:238870&theme=FEFU

4. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. дан. — Москва : ДМК Пресс, 2008. — 448 с. — Режим доступа: https://e.lanbook.com/book/3027

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Криптография», составляет 36 часов. На самостоятельную работу – 36 часов. При этом аудиторная нагрузка состоит из 10 лекционных часов и 26 лабораторных часов.

В рамках указанной дисциплины итоговой формы аттестации является зачет. Самостоятельная работа при подготовке к зачету включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для обеспечения данной дисциплины необходима аудитория, оснащенная презентационной техникой, компьютерный класс с программным обеспечением и возможностью использования Интернет-ресурсов, учебные и методические пособия (учебники, программы, сборники упражнений и т.д.), расходные материалы (бумага, картридж).

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**
Учебная аудитория для занятий семинарского типа 690922, Приморский край, г. Владивосток, остров Русский, полуостров	Комплект специализированной мебели: доска аудиторная – 1 шт.; парты – 30 шт.; стул -30 шт.; Проектор DLP, 3000 ANSI Lm, WXGA 1280x800, 2000:1 EW330U Mitsubishi,; Системный блок с монитором. Процессор: Intel I5-8600k 3.6Ghz, оперативная память: 32gb, жесткий диск: 1ТБ, графический ускоритель: Nvidia GTX 1080 Беспроводные

Саперный, поселок Аякс, 10 Здание ФЭК корпус А, лит О, ауд. G468	ЛВС для обучающихся обеспечены системой на базе точек доступа 802.11a/b/g/n 2x2 MIMO(2SS).

Приложение 1

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

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Криптография»
Направление подготовки
09.04.01 Информатика и вычислительная техника
Магистерская программа
«Кибербезопасность»
Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 неделя обучения	Подготовка лабораторных работ.	26	Отчет по лабораторной работе
2	Сессия	Подготовка к зачету	10	Зачет

Методические рекомендации к работе с литературными источниками

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы

1. Просмотр и проверка выполнения самостоятельной работы преподавателем.

2. Самопроверка, взаимопроверка выполненного задания в группе.

3. Обсуждение результатов выполненной работы на занятии.

4. Текущее тестирование.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентов учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;
- умение сформировать свою позицию, оценку и аргументировать ее

Критерии оценки выполнения контрольных заданий для самостоятельной работы

Процент правильных ответов	**Оценка**
От 95% до 100%	отлично
От 76% до 95%	хорошо
От 61% до 75%	удовлетворительно
Менее 61 %	неудовлетворительно

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников, материалов по практическим занятиям и лабораторным работам.

Задачи для самостоятельного решения

1. Докомпьютерная криптография:Показать, что нод(a,|A|)=1 н. и д. для однозначности дешифрования шифра c= a* m+b (mod |A|).

2. Докомпьютерная криптография:Описать обратное преобразование для модулярного шифра с a/=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 шифрованном тексте.

6. Докомпьютерная криптография:Расшифровать заданное сообщение ymjkwjvzjshdrjymtisjjixqt slhnumjwyjcyxytbtwp 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 шифрованном тексте).

9. Докомпьютерная криптография : Каким необходимым и достаточным условиям должен удовлетворять определитель матрицы E для того, чтобы преобразование Хилла c=E m+s (mod |A|), c, m, s - n-мерные векторы, E - n*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 B^n, B={0,1}.

12. Докомпьютерная криптография: Сколько существует нелинейных криптопреобразований B^3->B^3?

13. Докомпьютерная криптография: Доказать, что энтропия скалярного источника дискретных сообщений, заданного вероятностями p_1,...,p_n, принимает максимальное значение т. и т. т., когда все p_i, i=1,..,n, совпадают. (Известно, что если некоторая функция h_n от p_1,...,p_n непрерывна по совокупности переменных и обладает дополнительно тремя свойствами: 1) ее максимум достигается при равных p_i, i=1,..,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,...,p_n,0)=h_{n}(p_1,...,p_n), то h_n необходимо имеет вид шенноновской энтропии: h_{n}(p_1,...,p_n)=-\lambda \sum_{i=1}^{n} p_i \logp_i, где \lambda>0).

14. Докомпьютерная криптография: Доказать свойство иерархическойаддитивности 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. Testingimplementationsof 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 дополнительности DES (1): если C=DES(M,K), то C'=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^s=2^i, i=1, 2, … , 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=pq. Показать, что и при нод(n,w)/=1 расшифрование RSA сводится к возведению в степень d.

23. Пусть p=P[нод(a,b)=1, где a,b - два выбранные наугад числа].
- Доказать, что P[нод(a,b)=d, где a,b - два выбранные наугад числа] =p/d^2.
- Доказать, что \sum{d>=1} P[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)mod 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?

Приложение 2

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

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Криптография»
Направление подготовки
09.04.01 Информатика и вычислительная техника
Магистерская программа
«Кибербезопасность»
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции
ОПК-2. Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.1 Знать: современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач ОПК-2.2 Уметь: обосновывать выбор современных информационно-коммуникационных и интеллектуальных технологий, разрабатывать оригинальные программные средства для решения профессиональных задач ОПК-2.3 Владеть: навыками разработки оригинальных программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий, для решения профессиональных задач
ОПК-7. Способен адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий	ОПК-7.1 Знать: функциональные требования к прикладному программному обеспечению для решения актуальных задач предприятий отрасли, национальные стандарты обработки информации и автоматизированного проектирования ОПК-7.2 Уметь: приводить зарубежные комплексы обработки информации в соответствие с национальными стандартами, интегрировать с отраслевыми информационными системами ОПК-7.3 Владеть: навыками настройки интерфейса, разработки пользовательских шаблонов, подключения библиотек, добавления новых функций
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	ПК-2.1 Знает: модели безопасности компьютерных сетей; виды политик безопасности компьютерных систем и сетей; нормативно-правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации; организационные меры по защите информации ПК-2.2 Умеет: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей; разрабатывать профили защиты компьютерных систем; формулировать задания по

	безопасности компьютерных систем ПК-2.3 Владеет: навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; разработки руководящих документов по защите информации в организации

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Лекция 1. Блочные симметричные итеративные шифры	ОПК-2, ОПК-7, ПК-2	знает	устный или письменный опрос студентов во время лекции по изучаемому материалу (УО-1); теоретические диктанты (ПР-2);	зачет
			умеет	решение задач по изучаемой теме на практических занятиях (ПР-11);	зачет
			владеет	Технические средства контроля (ТС)	зачет
2	Лекция 2. Элементы теории сложности вычислений.	ОПК-2, ОПК-7, ПК-2	знает	устный или письменный опрос студентов во время лекции по изучаемому материалу (УО-1); теоретические диктанты (ПР-2);	зачет
			умеет	решение задач по изучаемой теме на практических занятиях (ПР-11);	зачет
			владеет	Технические средства контроля (ТС)	зачет
3	Лекция 3. Криптосистемы с открытым ключом	ОПК-2, ОПК-7, ПК-2	знает	устный или письменный опрос студентов во время лекции по изучаемому материалу (УО-1); теоретические диктанты (ПР-2);	зачет
			умеет	решение задач по изучаемой теме на практических	зачет

				занятиях (ПР-11);	
			владеет	Технические средства контроля (ТС)	зачет
4	Лекция 4. Аутентификация	ОПК-2, ОПК-7, ПК-2	знает	устный или письменный опрос студентов во время лекции по изучаемому материалу (УО-1); теоретические диктанты (ПР-2);	зачет
			умеет		зачет
			владеет		зачет
5	Лекция 5. Современные проблемы	ОПК-2, ОПК-7, ПК-2	знает	устный или письменный опрос студентов во время лекции по изучаемому материалу (УО-1); теоретические диктанты (ПР-2);	зачет
			умеет		
			владеет		

Оценочные средства для промежуточной аттестации
Список вопросов на зачет

1. Симметричные криптосистемы, перестановки и подстановки, одноалфавитные и многоалфавитные криптосистемы, потоковые и блочные шифры.
2. Протокол взаимной аутентификации. Схема обмена ключами Диффи-Хеллмана.
3. DES, двойной DES.
4. Тройной DES.
5. Группы, кольца, области целостности, поля.
6. Криптосистемы, базирующиеся на задаче о рюкзаке.
7. Обмен ключами по алгоритму BB84 (квантовая криптография).
8. RSA.
9. Шифр простой замены
10. Перестановочные шифры
11. Аффинные шифры над конечными полями
12. Мультипликативная группа кольца вычетов
13. Алгебраическая модель шифра
14. Вероятностная модель шифра

15. Шифр Виженера
16. Энтропия и избыточность языка
17. Теоретическая и практическая стойкость шифров
18. Имитостойкость шифров 11 .Блочные шифры
19. Линейные рекуррентные последовательности
20. Поточные шифры и генераторы ключевых последовательностей
21. Проблема факторизации в целых числах и шифр RSA.
22. Шифр Эль Гамаля.
23. Хеш функции.
24. Протоколы аутентификации.
25. Цифровые подписи
26. Алгоритм DES
27. Генератор ключевой последовательности A5
28. Анализ стойкости протоколов в неклассических логиках

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

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! .

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

1. Найдите наименьшее общее кратное систем чисел:

а) 720 и 1512 (по формуле);

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

2. Найдите число делителей, сумму делителей и значение функции Эйлера для числа n=343343.

3. Дано: ф(п) = 3600, $n = 3^a \cdot 5^e 11^y$. Найдите n.

4. Найдите две последние цифры числа 17^{61}.

5. Решите сравнение:

а) 12x = 4 (mod 5), б) 49x = 14 (mod 77).

о г, ~Гx = 7 (mod 17);

6. Решите систему сравнений: <

[x = 3 (mod 14).

7. Докажите, что если (a, b) = 1, то наибольший общий делитель чисел a + b и a^1 + b^2 равен либо 1, либо 2.

8. Докажите, что 53^{53} - 33^{33} делится на 10.

2 вариант

1. Найдите каноническое представление числа: а) 97363981 ; б) 19! .

~ Г X = 4 (mod 15);

8. Решите систему сравнений: <

[x = 13 (mod 21).

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).

---

1 Найдите наибольший общий делитель систем чисел:

а) 105369 и 4991 (по алгоритму Евклида);

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: ф(п) = 360, n = $3^a \cdot 5^e$. Найдите n.
6. Найдите две последние цифры числа 1 1^{203}.
7. Решите сравнение:
а) 24x = 6 (mod 25), б) 45x = 105 (mod 115).
о г, ~ Г x = 7 (mod 15);
8. Решите систему сравнений: <
[x = 11 (mod 25).
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 п = 2 оба числа простые).
4 вариант
1. Найдите каноническое представление числа:
а) 71899443; б) 31!
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 = 29 (mod 105), б) 56x = 16 (mod 116).
8. Решите систему сравнений: x = 3 (mod 35); x = 18 (mod 55); x = 24 (mod 91).
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 индивидуальных домашних заданий Тема: Метод резолюций в алгебре высказываний
Проверить истинность следующих соотношений (3-мя способами):
1. A|= AvC,
2. A ^ B , C | = A ^ C ,
3. A^B,в|=A.

Тема: Логика предикатов

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

^ ((ЗхV^(х, *у) v* Зх3уY(х, *у))* л Зх3_уX(х, *у))*

2. Записать формулу Ф(х,_у^), истинную в <N;+,-> тогда и только тогда, когда: z = НОК *(ху)*

3. Записать формулу Ф(х), истинную в <N;+,-> тогда и только тогда, когда: х - простое число.

4. Пусть ф, ^, X - атомарные формулы логики предикатов. Привести следующую формулу логики предикатов к пренексной нормальной форме

^((ЗхV^(х,*у) ^ 3х3у4*(х,*у))л Ух 3у*^X(х,*у))*

Тема: Исчисление предикатов

Пусть Ф , ^, X, © - формулы исчисления предикатов. Построить вывод формулы исчисления предикатов из данного множества гипотез.

Тема: Частично рекурсивные функции

Доказать, что следующие функции примитивно рекурсивны:

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

Доказать, что следующие функции частично рекурсивны:

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

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

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: $ф(5^x) = 2500$.

6. Найдите две последние цифры числа 7^{114}.

7. Решите сравнение:

а) 13х = 5 (mod 21), б) 88х = 14 (mod 26).

2. Найдите наибольший общий делитель систем чисел: