МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2023

Рабочая программа дисциплины (модуля) «Методы и средства криптографической защиты информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Шумик Е.Г., кандидат экономических наук, доцент, Кафедра математики и моделирования, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от «____»_____20__г. , протокол № _____

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)
Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000BBD6E5
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью преподавания дисциплины вляется изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины - дать основы:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- принципов синтеза и анализа шифров;

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-10 : Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1к : понимает основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	РД4	Знание	Особенности проведения проверок работоспособности криптографических средств защиты информации
		ОПК-10.2к : обладает методиками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	РД6	Навык	проведения проверок работоспособности криптографических средств защиты информации
	ОПК-15 : Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1к : перечисляет этапы разработки политики информационной безопасности для организации; особенности подсистем защиты ОС Windows и Linux; стандартные средства организации виртуальных частных сетей	РД1	Знание	современную научно-техническую литературу в области криптографической защиты
			РД2	Умение	Систематизировать нормативно-правовую документацию в области криптографии

			РД3	Навык	изучения научно-технической информации, в том числе на иностранном языке
	ОПК-2 : Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.2к : использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	РД5	Умение	проводить проверки работоспособности криптографических средств защиты информации
	ОПК-9 : Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.3к : оценивает работоспособность сетевых проектов; исследует характеристики сетевой активности созданных проектов	РД7	Знание	модели шифров и математические методы их исследования
			РД8	Умение	применять математические методы описания и исследования криптографических систем
			РД9	Навык	математического моделирования в криптографии

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Методы и средства криптографической защиты информации» относится к базовой части учебного плана специальности 10.05.03

«Информационная безопасность автоматизированных систем».

Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Алгебра и геометрия», «Математический анализ модуль 1». На данную дисциплину опираются «Криптографические протоколы».

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	7	5	91	36	36	0	1	18	89	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Введение в криптографию	РД1, РД2, РД3	6	6	0	3	практическое задание
2	Основные классы шифров и их свойства	РД5, РД6	6	6	0	3	практическое задание
3	Надежность шифров	РД4, РД5, РД6	6	6	0	3	практическое задание
4	Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии	РД5, РД6, РД7, РД8, РД9	6	6	0	3	практическое задание
5	Современные системы шифрования	РД4, РД7, РД8, РД9	6	6	0	3	практическое задание
6	Общие вопросы	РД1, РД2, РД3, РД4	6	6	0	3	практическое задание
Итого по таблице			**36**	**36**	**0**	**18**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Введение в криптографию.

Содержание темы: Основные методы защиты информации. Из истории криптографии. Открытые сообщения и их характеристики. Частотные характеристики открытых сообщений. Математические модели открытых сообщений. Критерии на открытый текст. Способы представления информации, подлежащей шифрованию. Особенности не текстовых сообщений. Основные понятия криптографии. Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам. Принципы организации шифрованной связи. Понятие криптосистемы. Симметричные и асимметричные криптосистемы. Вопросы распределения ключей в сети шифрованной связи.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Основные классы шифров и их свойства.

Содержание темы: Шифры перестановки. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. Шифры замены. Одноалфавитные и многоалфавитные замены. Поточные и блочные шифры замены. DES и ГОСТ 28147-89. Криптоанализ шифров замены. Шифры гаммирования. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому

занятию.

Тема 3 Надежность шифров.

Содержание темы: Теория К. Шеннона. Теоретико-информационный подход к оценке стойкости шифров. Ненадежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Избыточность языка и расстояние единственности. Имитостойкость шифров. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации и ортогональные конфигурации. Помехоустойчивость шифров. Помехоустойчивое кодирование. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии.

Содержание темы: Методы матстатистики в криптографии. Элементы матстатистики: матожидание и дисперсия случайной величины, схема Бернулли, формула биномиального распределения, полиномиальная схема, формула полиномиального распределения, формула Пуассона, нормальное распределение, центрирование, нормирование, «хи-квадрат» распределение, утверждение о выборочной дисперсии, центральная предельная теорема. Построение статистического критерия. Статистические критерии для проверки гипотез о случайности и однородности текстов. 7 практических формул. 5 базовых тестов на случайность битовой последовательности. Стандарт FIPS 140. Специальные вопросы теории двоичных функций Понятие булевой функции. Вес функции. СДНФ, СКНФ, многочлен Жегалкина. Представление двоичной функции многочленом с действительными коэффициентами. Представление двоичных функций рядом Фурье. Вероятностная функция. К-выравнивающая функции. Статистический аналог функции. Статистическая структура двоичной функции. Определение статистической структуры методом быстрого преобразования Фурье. Понятие линейного криптоанализа. Весовая структура двоичной функции. К-равновероятная двоичная функция. Совершенная нелинейность. Понятие дифференциального криптоанализа. Элементы теории ЛРП, используемые в криптографии. Определение ЛРП. LR(F), базис LR(F). Понятие генератора ЛРП. Характеристический и минимальные многочлены ЛРП. Вычисления минимального многочлена через характеристический многочлен и генератор ЛРП. Длина подхода, период последовательности. Длина подхода и период многочлена над полем. Понятие примитивного многочлена. Критерий примитивности неприводимого многочлена. Теорема о случайности k-грамм в ЛРП максимального периода .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 5 Современные системы шифрования.

Содержание темы: Блочное шифрование. Сети Фейстеля. Схема шифрования DES. 3DES, DESX. Схема шифрования ГОСТ – 28147-89. Различия между DES и ГОСТ. Шифр AES Основные режимы блочного шифрования. Поточные системы шифрования. Синхронные системы и системы с самосинхронизацией. Принципы построения поточных систем. Управляющий и шифрующий блоки. Линейный конгруэнтный генератор. Генераторы с неполиномиальной зависимостью. ЛРС. Требования к управляющему блоку.

Требования к шифрующему блоку. Схема шифрсистемы A5. Шифрсистема Гиффорда. Фильтрующие генераторы. Комбинирующие генераторы. Композиция ЛРС. Схемы с динамическим изменением закона рекурсии. Генераторы Макларена-Марсальи. Методы анализа криптографических алгоритмов. Алгоритмические, аналитические и статистические методы криптоанализа поточных шифров. Особенности криптоанализа блочных шифров.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 6 Общие вопросы.

Содержание темы: Обзор стандартов в криптографии. Международные стандарты (ISO, ISO/IEC). Государственные стандарты России (ГОСТ). Американские стандарты (ANSI). Государственные стандарты США (FIPS). RFC и PKCS. Причины взлома криптосистем. Основные ошибки при создании и использовании криптосистем, приводящие к взлому криптосистемы. Право, экспорт, ведомства. Ведомства, функционирующие в криптографической сфере. Экспортные ограничения в области криптографии. Правовые нормы. Заключение. Проблемы и перспективы исследований в области современной криптографии. Нерешенные задачи. Итоги изучения курса.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Гисин, В. Б. Криптография и распределенные реестры : учебное пособие / В. Б. Гисин. - Москва : Прометей, 2022. - 186 с. - ISBN 978-5-00172-257-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/2124870 (дата обращения: 14.12.2023).
2. Донгак, Ш. М. Криптография : учебное пособие / Ш. М. Донгак. — Москва : РТУ МИРЭА, 2021 — Часть 3— 2021. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182517 (дата обращения: 28.02.2024). — Режим доступа: для авториз. пользователей.
3. Каширская, Е. Н. Основы криптографического анализа : учебное пособие / Е. Н. Каширская. — Москва : РТУ МИРЭА, 2020. — 74 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163805 (дата обращения: 28.02.2024). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Донгак, Ш. М. Криптография: Практикум : учебное пособие / Ш. М. Донгак. — Москва : РТУ МИРЭА, 2020 — Часть 2— 2020. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163935 (дата обращения: 28.02.2024). — Режим доступа: для авториз. пользователей.
2. Фомичев, В. М. Криптография — наука о тайнописи : учебное пособие / В. М. Фомичев. - Москва : Прометей, 2020. - 66 с. - ISBN 978-5-00172-040-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1851305 (дата обращения: 01.03.2023). – Режим доступа: по подписке.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Электронно-библиотечная система "ZNANIUM.COM"
2. Электронно-библиотечная система "ZNANIUM.COM" - Режим доступа: https://znanium.com/
3. Электронно-библиотечная система "ЛАНЬ"
4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
5. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
6. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

· Компьютеры
· Проектор

Программное обеспечение:

· Microsoft Office Standard 2007 Russian
· Office

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность и специализация

10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2023

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-10 : Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1к : понимает основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности
		ОПК-10.2к : обладает методиками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности
	ОПК-15 : Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1к : перечисляет этапы разработки политики информационной безопасности для организации; особенности подсистем защиты ОС Windows и Linux; стандартные средства организации виртуальных частных сетей
	ОПК-2 : Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.2к : использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности
	ОПК-9 : Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.3к : оценивает работоспособность сетевых проектов; исследует характеристики сетевой активности созданных проектов

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-2 «Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	

ОПК-2.2к : использует современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	РД 5	Умение	проводить проверки работоспособности криптографических средств защиты информации	выполнение практических заданий

Компетенция ОПК-9 «Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-9.3к : оценивает работоспособность сетевых проектов; исследует характеристики сетевой активности созданных проектов	РД 7	Знание	модели шифров и математические методы их исследования	решение тестовых заданий
	РД 8	Умение	применять математические методы описания и исследования криптографических систем	выполнение практических заданий
	РД 9	Навык	математического моделирования в криптографии	выполнение практических заданий

Компетенция ОПК-10 «Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности»

Таблица 2.3 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-10.1к : понимает основные принципы построения средств криптографической и технической защиты информации и для решения задач профессиональной деятельности	РД 4	Знание	Особенности проведения проверок работоспособности криптографических средств защиты информации	решение тестовых заданий

ОПК-10.2к : обладает методиками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	РД6	Навык	проведения проверок работоспособности криптографических средств защиты информации	выполнение практических заданий

Компетенция ОПК-15 «Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем»

Таблица 2.4 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-15.1к : перечисляет этапы разработки политики информационной безопасности для организации; особенности подсистем защиты ОС Windows и Linux; стандартные средства организации виртуальных частных сетей	РД1	Знание	современную научно- техническую литературу в области криптографической защиты	решение тестовых заданий
	РД2	Умение	Систематизировать нормативно-правовую документацию в области криптографии	выполнение практических заданий
	РД3	Навык	изучения научно- технической информации, в том числе на иностранном языке	выполнение практических заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : современную научно- техническую литературу в области криптографической защиты	1.1. Введение в криптографию	Тест	Опрос
		1.6. Общие вопросы	Тест	Опрос
РД2	Умение : Систематизировать нормативно-правовую документацию в области криптографии	1.1. Введение в криптографию	Практическая работа	Опрос

		1.6. Общие вопросы	Практическая работа	Опрос
РД3	Навык : изучения научно- технической информации, в том числе на иностранном языке	1.1. Введение в криптографию	Практическая работа	Опрос
		1.6. Общие вопросы	Практическая работа	Опрос
РД4	Знание : Особенности проведения проверок работоспособности криптографических средств защиты информации	1.3. Надежность шифров	Тест	Опрос
		1.5. Современные системы шифрования	Тест	Опрос
		1.6. Общие вопросы	Тест	Опрос
РД5	Умение : проводить проверки работоспособности криптографических средств защиты информации	1.2. Основные классы шифров и их свойства	Практическая работа	Опрос
		1.3. Надежность шифров	Практическая работа	Опрос
		1.4. Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии	Практическая работа	Опрос
РД6	Навык : проведения проверок работоспособности криптографических средств защиты информации	1.2. Основные классы шифров и их свойства	Практическая работа	Опрос
		1.3. Надежность шифров	Практическая работа	Опрос
		1.4. Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии	Практическая работа	Опрос
РД7	Знание : модели шифров и математические методы их исследования	1.4. Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии	Тест	Опрос
		1.5. Современные системы шифрования	Тест	Опрос
РД8	Умение : применять математические методы описания и исследования криптографических систем	1.4. Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии	Практическая работа	Опрос
		1.5. Современные системы шифрования	Практическая работа	Опрос
РД9	Навык : математического моделирования в криптографии	1.4. Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии	Практическая работа	Опрос
		1.5. Современные системы шифрования	Практическая работа	Опрос

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности		Оценочное средство		
	Тест 1-5	Практические занятия	Экзамен	Итого
Лекционные занятия	20			80
Практическая работа		60		
Промежуточная аттестация			20	20
Итого	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, об наруживает всестороннее, систематическое и глубокое знание учебного матер иала, усвоил основную литературу и знаком с дополнительной литературой, ре комендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниям и, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: ос новные знания, умения освоены, но допускаются незначительные ошибки, нет очности, затруднения при аналитических операциях, переносе знаний и умени й на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в х оде контрольных мероприятий допускаются значительные ошибки, проявляетс я отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарн ым компетенциям, студент испытывает значительные затруднения при оперир овании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недо статочность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Контрольный тест

1. Конфиденциальность защищаемой информации обеспечивается с помощью...
- электронной подписи
- шифрования
- хэш-функци

2. Способность шифра противостоять попыткам противника по имитации или подмене зашифрованной информации называется
- имитостойкостью.
- криптостойкостью.
- помехозащищенностью

3. Если криптоаналитик может взломать шифр, но не обладает необходимыми

вычислительными ресурсами, то считается, что

- шифр является практически стойким.
- шифр является теоретически стойким.
- шифр является практически имитостойким.

4. Если для шифрования и расшифрования используется один и тот же ключ, то шифр является

- симметричным.
- ассиметричным.
- блочным.

5. Шифры, в которых знание ключа шифрования не позволяет определить ключ расшифрования называются

- поточными.
- симетричными.
- ассиметричными.

6. Шифры, в которых каждый символ открытого текста зашифровывается независимо от других называются

- блочными.
- имитозащищенными.
- поточными.

7. Шифрование информации предназначено для обеспечения

- целостности защищаемой информации
- конфиденциальности защищаемой информации
- доступности защищаемой информации

8. Исходные данные с доступным семантическим содержанием, подлежащие криптографическому преобразованию, называются

- открытый текст
- шифртекст
- имитовставка

9. Параметр шифра, определяющий выбор конкретного варианта преобразования зашифрования или расшифрования из множества преобразований, составляющих шифр, называется…

- алгоритм
- шифр
- ключ

10. Процесс преобразования шифртекста в открытый текст при неизвестном ключе называется…

- дешифрование
- зашифрование
- расшифрование

11. Если за один такт шифрования преобразованию подвергается группа знаков открытого текста, то такой шифр называется

- блочным
- поточным
- ассиметричным

12. На основе сети Фейстеля построен алгоритм шифрования

- AES
- ГОСТ 28147
- RC4

13. Режим использования блочного шифра, при котором блочный шифр может использоваться как поточный называется

- режим простой замены со сцеплением.
- режим гаммирования с обратной связью
- режим простой замены.

14 Режим простой замены заключается в обработке блоков открытого текста независимо от других обработку блоков открытого текста в зависимости от результата зашифрования

- предыдущего блока
- обработку блоков открытого текста в режиме наложения гаммы

14. Шифр называется блочным, если…

- за один такт шифрования преобразованию подвергается группа знаков открытого текста
- за один такт шифрования преобразованию подвергается один знак открытого текста
- группа знаков открытого текста преобразуется за несколько тактов шифрования

15. Если управляющая гамма поточного шифра зависит только от ключа и не зависит от открытого текста и шифротекста, то такой шифр называется

- синхронным.
- самосинхронизирующимся.
- независимым.

16. Достоинством поточных шифров по сравнению с блочными является

- наличие открытого ключа
- высокая стоимость реализации
- высокая скорость работы

17. Недостатком генераторов псевдослучайных последовательностей является

- сложность реализации
- зависимость от параметров окружающей среды
- периодичность последовательности

18. Если управляющая гамма поточного шифра зависит от ключа и от открытого текста и шифротекста, то такой шифр называется

- синхронным.
- самосинхронизирующимся.
- независимым.

19. В алгоритме ГОСТ 34.12-15 размера блока составляет

- 64 бита
- 128 бит, 192 бита и 256 бит
- 64 бита и 128 бит

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, помнению студента, вариант ответа. В течение семестра проводится 6 тестов по 6 темам на лекционных занятиях, в каждом тесте 16 вопросов.

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Студент допустил не более 2х ошибок
4	5-7	Студент совершил от 3 до 6 ошибок в ответах на тест
3	3-4	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-2	Студент совершил 11 и более ошибок в ответах на тест

5.2 Примеры заданий для выполнения практических работ

Практическая работа 1.

Разработать алгоритм и составить программу, позволяющую закодировать любой текст одним из вышеизложенных методов и выполнить обратное преобразование.

Метод, которым необходимо зашифровать исходную информацию, выбирается преподавателем.

Язык программирования выбирается произвольно.

2. Осуществить вывод на экран или принтер полученной криптограммы.

3. Провести дешифрование данной криптограммы, в результате должен быть получен исходный текст.

4. Результаты работы оформить в виде отчета.

Практическая работа 2.

1Взять у преподавателя параметры генератора ПСЧ: A, C, T0, b.

2. Разработать программу шифрования и дешифрования текста.

3. Произвести шифрование исходного текста, получить шифрограмму, осуществить ее дешифрование и сравнение с исходным текстом. Рекомендуется для представления символов исходного текста использовать стандартную кодировку символов.

4. Произвести изменение одного или несколько параметров генератора случайных чисел, осуществить получение шифрограммы и сравнение ее с предыдущим вариантом.

5. Результаты работы оформить в виде отчета.

Практическая работа 3.

1 Взять у преподавателя параметры сети Фейштеля.

2. Разработать программу шифрования и дешифрования текста блоками, В программе предусмотреть ввод криптографического ключа, вычисление образующей функции, зависящей от материала ключа и части блока.

3. Произвести шифрование исходного текста, получить шифрограмму, осуществить ее дешифрование и сравнение с исходным текстом.

4. Результаты работы оформить в виде отчета

Практическая работа 4.

1. Разработать программу, осуществляющую шифрование и дешифрование сообщения алгоритмом RSA. Ключи генерируются на основе чисел p и q, значения взять у преподавателя. При выборе числа e использовать минимально возможное

2. Исходное сообщение M может состоять из символов. как русского, так и любого другого алфавита.

3. Обеспечить вывод ключей и зашифрованного текста.

4. В программе предусмотреть проверку, являются ли два числа взаимно простыми.

5. Результаты работы оформить в виде отчета.

Практическая работа 5

1. Взять у преподавателя алгоритм вычисления хэшфункции (контрольной суммы).
2. Реализовать программную реализацию алгоритма создания и проверки электронно-цифровой подписи.
3. Подписать текстовое сообшение
4. Проверить правильность ЭЦП.
5. Внести измененя в сделанную подпись. Убедится, что подпись не является подлинной.
6. Результаты работы оформить в виде отчета.

Краткие методические указания

На выполнение одной практической работы отводится не менее трех двухчасовых занятий. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме.

Шкала оценки

Оценка	Баллы	Описание
5	15-19	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	10-14	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	4-9	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.

2	0-3	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/или неверно применил методы необходимые его выполнения.

5.3 Примерные темы для опроса

1. История развития криптографии
2. Основные понятия
3. Модели шифров и открытых текстов. Критерии распознавания открытых текстов
4. Шифры замены. Обобщенная модель. Алгоритм Якобсона.
5. Шифры перестановки и методы их вскрытия.
6. Дисковые шифры.

7. Шифры гаммирования. Возможность восстановления вероятности знаков гаммы. Восстановление текстов при неравновероятной гамме.

8. Повторное использование гаммы. Использование неисправности в реализации шифра Вернама.

9. Криптоанализ шифра Виженера. Ошибка шифровальщика (пропуск участка открытого текста).

10. Энтропия. Избыточность. Формула неопределенности шифра по ключу. Теорема о числе ложных ключей. Расстояние единственности

11. Стойкость шифров. Виды криптоатак. Совершенный шифр. Утверждение о совершенном шифре. Теорема Шеннона о совершенном шифре. Примеры совершенных шифров. Практическая стойкость.

12. Имитостойкость. Совершенная имитостойкость. Помехоустойчивость. Шифры, не распространяющие искажений, изометрии. Теорема Марков

13. Статистика в криптографии.

14. Тесты на случайность битовой последовательности.

15. Сети Фейстеля. Схема шифрования DES. 3DES, DESX. 4 основных режима блочного шифрования.

16. Схема шифрования ГОСТ – 28147-89. Различия между DES и ГОСТ.

17. Шифр AES.

18. Понятие булевой функции. Виды представлений булевой функции (СДНФ, СКНФ, многочлен Жегалкина, многочлен с действительными коэффициентами, ряд Фурье).

19. Понятие статистического аналога и статистической структуры двоичной функции. Определение статистической структуры методом быстрого преобразования Фурье. Линейный криптоанализ.

20. Понятие вероятностной функции. k-выравнивающая и k-равновероятная двоичная функция. Понятие совершенной нелинейности.

21. Определение ЛРП. Понятие генератора и минимального многочлена ЛРП. Формула вычисления минимального многочлена через характеристический многочлен и генератор ЛРП.

22. Длина подхода и период последовательности и многочлена над полем. Критерий примитивности неприводимого многочлена. Теорема о случайности к-грамм в ЛРП максимального периода

23. Синхронные системы и системы с самосинхронизацией. Принципы построения поточных систем. Управляющий и шифрующий блоки. Линейный конгруэнтный генератор. Генераторы с неполиномиальной зависимостью. ЛРС. Требования к управляющему блоку и шифрующему блоку.

24. Схема шифрсистемы А5. Шифрсистема Гиффорда. Фильтрующие генераторы. Комбинирующие генераторы

25. Композиция ЛРС. Схемы с динамическим изменением закона рекурсии. Генераторы Макларена- Марсальи

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.