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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

Добржинский Ю.В
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптографические методы защиты информации
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс 4 семестр 7
лекции 36 час.
практические занятия 108 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек. 9 / пр. 36 / лаб. 00 час.
всего часов аудиторной нагрузки 144 час.
в том числе с использованием МАО 45 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 45 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 7 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 01.12.2016 № 1512

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 10 от « 15 » июня 2019 г.

И.о. заведующего кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель: Гончаров С.М., к.ф.-м.н, доцент

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

ABSTRACT

Specialist's degree in *10.05.01 Computer Security*

Specialization "*Mathematical Methods for Information Security*"

Course title: *Cryptographic methods of information protection*

Basic part of Block , _6_credits

Instructor: *Goncharov S.M.*

At the beginning of the course a student should be able to:

- the ability to correctly apply in solving professional problems the apparatus of mathematical analysis, geometry, algebra, discrete mathematics, mathematical logic, theory of algorithms, probability theory, mathematical statistics, information theory, number-theoretic methods (OPK-2);
- the ability to develop formal models of security policies, access control and information flow policies in computer systems, taking into account information security threats (OPK-9).

Learning outcomes:

- (OPK-4) the ability to apply the methodology of scientific research in professional activities, including in the work on interdisciplinary and innovative projects
- (OPK-10) the ability to build an algorithm independently, to conduct its analysis and implementation in modern software systems

Course description: *This discipline covers such issues as the basic methods of information security, the basic concepts of cryptography, the principles of the organization of encrypted communication, the main classes of ciphers and their properties.*

Main course literature:

1. Орлов, В.А. Теория чисел в криптографии [Электронный ресурс] : учебное пособие / В.А. Орлов, Н.В. Медведев, Н.А. Шимко, А.Б. Домрачева. — Электрон. дан. — Москва : МГТУ им. Н.Э. Баумана, 2011. — 223 с. — Режим доступа: https://e.lanbook.com/book/106532.

2. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192.

3. Панкратова, И.А. Булевы функции в криптографии [Электронный ресурс] : учебное пособие / И.А. Панкратова. — Электрон. дан. — Томск : ТГУ, 2014. — 88 с. — Режим доступа: https://e.lanbook.com/book/76702.

4. Серёдкин, А.Н. Основы защиты информации и информационные технологии. В 3 частях. Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ [Электронный ресурс] : учебное пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза : ПензГТУ, 2013. — 180 с. — Режим доступа: https://e.lanbook.com/book/62755.

Form of final control: *exam*

Аннотация к рабочей программе дисциплины «Криптографические методы защиты информации»

Курс учебной дисциплины «Криптографические методы защиты информации» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.6.5.

Общая трудоемкость дисциплины в зачетных единицах составляет 6 з.е., в академических часах – 216 часов (лекции – 36 часов, практические занятия – 108 часов, самостоятельная работа – 72 часа, в том числе 45 часов на подготовку к экзамену). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина логически и содержательно связана с такими курсами, как «Теоретико-числовые методы в криптографии», «Криптографические протоколы».

Данная дисциплина затрагивает такие вопросы, как основные методы защиты информации, основные понятия криптографии, принципы организации шифрованной связи, основные классы шифров и их свойства.

Цель дисциплины - изложить основополагающие принципы 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;

- изучение принципов синтеза и анализа шифров;

- ознакомление с математическими методами, используемых в криптоанализе.

Для успешного изучения дисциплины «Криптографические методы защиты информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);

- способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9).

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

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-4) способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знает	методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
	Умеет	применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
	Владеет	методикой и методологией научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
(ОПК-10) способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Знает	современные языки программирования и программные комплексы
	Умеет	строить алгоритмы
	Владеет	способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах

Для формирования вышеуказанных компетенций в рамках дисциплины «Криптографические методы защиты информации» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах.

Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Введение в криптографию (6 час.)

Тема 1. Основные методы защиты информации (1 час.)

Требования к защите информации, оценка возможностей противоборствующей стороны. Методология разработки и анализа средств защиты. Классические модели защиты информации. Стеганографические и криптографические методы защиты информации.

Тема 2. Из истории криптографии (1 час.)

Краткий исторический очерк развития криптографии. Исторические примеры: шифр Цезаря, квадрат Полибия, шифр Виженера, шифр Сцитала, решетка Кардано, книжный шифр и др. Основные этапы становления криптографии как науки.

Тема 3. Открытые сообщения и их характеристики (1 час.)

Частотные характеристики открытых сообщений. Математические модели открытых сообщений. Критерии на открытый текст. Способы представления информации, подлежащей шифрованию. Особенности нетекстовых сообщений.

Тема 4. Основные понятия криптографии (1 час.)

Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.

Тема 5. Принципы организации шифрованной связи (2 час.)

Понятие криптосистемы. Симметричные и асимметричные криптосистемы. Вопросы распределения ключей в сети шифрованной связи.

Раздел II. Основные классы шифров и их свойства (6 час.)

Тема 1. Шифры перестановки (2 час.)

Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки.

Тема 2. Шифры замены (2 час.)

Одноалфавитные и многоалфавитные замены. Поточные и блочные шифры замены. DES и ГОСТ 28147-89. Криптоанализ шифров замены.

Тема 3. Шифры гаммирования (2 час.)

Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.

Раздел III. Надежность шифров (4 час.)

Тема 1. Теория К.Шеннона (1 час.)

Теоретико-информационный подход к оценке стойкости шифров. Ненадежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Избыточность языка и расстояние единственности.

Тема 2. Имитостойкость шифров (1 час.)

Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации и ортогональные конфигурации.

Тема 3. Помехоустойчивость шифров (2 час.)

Помехоустойчивое кодирование. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.

Раздел VI. Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии (8 час.)

Тема 1. Методы матстатистики в криптографии (2 час.)

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.

Тема 2. Специальные вопросы теории двоичных функций (3 час.)

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 функция. 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.

Тема 3. Элементы теории ЛРП, используемые в криптографии (3 час.)

Определение ЛРП. $L_R(F)$, базис $L_R(F)$. 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.

Раздел V. Современные системы шифрования (6 час.)

Тема 1. Блочное шифрование (2 час.)

Сети Фейстеля. Схема шифрования DES. 3DES, DESX. Схема шифрования ГОСТ – 28147-89. Различия между DES и ГОСТ. Шифр AES Основные режимы блочного шифрования.

Тема 2. Поточные системы шифрования (2 час.)

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.

Тема 3. Методы анализа криптографических алгоритмов (2 час.)

Алгоритмические, аналитические и статистические методы криптоанализа поточных шифров. Особенности криптоанализа блочных шифров.

Раздел VI. Общие вопросы (6 час.)

Тема 1. Обзор стандартов в криптографии (1 час.)

Международные стандарты (ISO, ISO/IEC). Государственные стандарты России (ГОСТ). Американские стандарты (ANSI). Государственные стандарты США (FIPS). RFC и PKCS.

Тема 2. Причины взлома криптосистем (2 час.)

Основные ошибки при создании и использовании криптосистем, приводящие к взлому криптосистемы.

Тема 3. Право, экспорт, ведомства (2 час.)

Ведомства, функционирующие в криптографической сфере. Экспортные ограничения в области криптографии. Правовые нормы.

Тема 4. Заключение (1 час.)

Проблемы и перспективы исследований в области современной криптографии. Нерешенные задачи. Итоги изучения курса.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (108 час.)

Занятие 1. Освоение процессов зашифрования и расшифрования для простейших шифров (2 час)

1. Выполнение шифрования простейшими шифрами.
2. Выполнение расшифрования простейших шифров.

Занятие 2. Модели открытых текстов. Избыточность языка (2 час.)

1. Изучение и применение методов открытых текстов.
2. Избыточность языка, особенности.

Занятие 3. Вскрытие шифров замены с использованием статистических закономерностей открытых сообщений (2 час.)

1. Методы замены.
2. Использование шифров замены с использованием закономерностей открытых сообщений.
3. Вскрытие шифров замены.

Занятие 4. Вскрытие шифров перестановки (2 час.)

4. Методы перестановки.
5. Использование шифров перестановки.
6. Вскрытие шифров перестановки.

Занятие 5. Определение короткой гаммы по шифротексту (2 час.)

1. Инициализация.
2. Генерация гаммы.
3. Определение короткой гаммы.

Занятие 6. Бесключевое чтение на комплекте текстов, закрытых одной гаммой (2 час.)

Занятие 7. Надежность шифров. (2 час.)

Занятие 8. Построение конечного поля. Операции над элементами поля. (2 час.)

Занятие 9. Методы статистического анализа последовательностей (4 час.)

Занятие 10. Построение критериев открытого текста (1 час.)

Занятие 11. Блочное шифрование (2 час.)

Занятие 12. Представление двоичных функций (2 час.)

Занятие 13. Вычисление характеристик двоичных функций (1 час.)

Занятие 14. Построение статистических аналогов функций (2 час.)

Занятие 15. Вычисление периодов линейных рекуррентных последовательностей (4 час.)

Занятие 16. Современные системы шифрования (2 час.)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Криптографические методы защиты информации» 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	Раздел I. Введение в криптографию	ОПК-4 ОПК-10	знает	собеседование (ОУ-1)	1-7
			умеет	коллоквиум (ОУ-2)	1-7
			владеет	конспект (ПР-7)	1-7
2	Раздел II. Основные классы шифров и их свойства	ОПК-4 ОПК-10	знает	собеседование (ОУ-1)	8-10
			умеет	коллоквиум (ОУ-2)	8-10
			владеет	конспект (ПР-7)	8-10
3	Раздел III. Надежность шифров	ОПК-4 ОПК-10	знает	собеседование (ОУ-1)	11-19
			умеет	коллоквиум (ОУ-2)	11-19
			владеет	конспект (ПР-7)	11-19
4	Раздел VI. Методы математическо	ОПК-4 ОПК-10	знает	собеседование (ОУ-1)	20-25
			умеет	коллоквиум (ОУ-2)	20-25

	й статистики, теории булевых функций и теории линейных рекуррентных последователь ностей в криптографии		владеет	конспект (ПР-7)	20-25
5	Раздел V. Современные системы	ОПК-4 ОПК-10	знает	собеседова ние (ОУ-1)	
			умеет	коллоквиу м (ОУ-2)	
			владеет	конспект (ПР-7)	
6	Раздел VI. Общие вопросы	ОПК-4 ОПК-10	знает	собеседова ние (ОУ-1)	
			умеет	коллоквиу м (ОУ-2)	
			владеет	конспект (ПР-7)	

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и 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. Орлов, В.А. Теория чисел в криптографии [Электронный ресурс] : учебное пособие / В.А. Орлов, Н.В. Медведев, Н.А. Шимко, А.Б. Домрачева. — Электрон. дан. — Москва : МГТУ им. Н.Э. Баумана, 2011. — 223 с. — Режим доступа: https://e.lanbook.com/book/106532.

2. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192.

3. Панкратова, И.А. Булевы функции в криптографии [Электронный ресурс] : учебное пособие / И.А. Панкратова. — Электрон. дан. — Томск : ТГУ, 2014. — 88 с. — Режим доступа: https://e.lanbook.com/book/76702.

4. Серёдкин, А.Н. Основы защиты информации и информационные технологии. В 3 частях. Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ [Электронный ресурс] : учебное пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза : ПензГТУ, 2013. — 180 с. — Режим доступа: https://e.lanbook.com/book/62755.

Дополнительная литература

1. Серёдкин, А.Н. Основы защиты информации и информационные технологии. В 3 частях. Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ [Электронный ресурс] : учебное пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза : ПензГТУ, 2013. — 180 с. — Режим доступа: https://e.lanbook.com/book/62755.

2. Туганбаев, А.А. Теория вероятностей и математическая статистика [Электронный ресурс] : учебное пособие / А.А. Туганбаев, В.Г. Крупин. — Электрон. дан. — Санкт-Петербург : Лань, 2011. — 320 с. — Режим доступа: https://e.lanbook.com/book/652.

3. Боровков, А.А. Математическая статистика [Электронный ресурс] : учебник / А.А. Боровков. — Электрон. дан. — Санкт-Петербург : Лань, 2010. — 704 с. — Режим доступа: https://e.lanbook.com/book/3810.

4. Кукина, Е.Г. Введение в криптографию: сборник задач и упражнений [Электронный ресурс] / Е.Г. Кукина, В.А. Романьков. — Электрон. дан. — Омск : ОмГУ, 2013. — 91 с. — Режим доступа: https://e.lanbook.com/book/75394.

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 945, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	"1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16

	лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019." 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Криптографические методы защиты информации», составляет 216 академических часов. На самостоятельную работу – 72 часа. При этом аудиторная нагрузка состоит из 36 лекционных часов и 108 часов практических занятий.

Обучающийся получает теоретические знания на лекционных занятиях, необходимые для последующего выполнения практических заданий. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

При подготовке к практическим занятиям также необходимо повторить теоретический материал.

Промежуточная форма аттестации по данной дисциплине – зачет. Вопросы к зачету соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к зачету студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 945, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 24) Оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800

	Сетевая видеокамера Multipix MP-HD718", доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт

Приложение 1

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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Криптографические методы защиты информации»
Специальность 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 недели обучения	Выполнение практических занятий. (Отчет по практическим занятиям 1-9)	27	Отчет о выполнении
8	Сессия	Подготовка к экзамену	45	Экзамен

Материалы для самостоятельной работы студентов

Основу методического обеспечения изучения дисциплины составляют учебники, материалы к лекциям в электронном виде и методические указания к выполнению практических заданий и лабораторного практикума.

Список библиографических источников:

1. Алферов А.П., Зубов А.Ю.,Кузьмин А.С.,Черемушкин А.В. Основы криптографии. М.: «Гелиос АРВ», 2002.

2. Бабаш А.В., Шанкин Г.П., Криптография, М.: СОЛОН-Р, 2002.

3. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их криптоанализа. М.: «Гелиос АРВ», 2006.

4. С.Баричев, Р.Серов. Основы современной криптографии. М.: 2002.

5. Гончаров С.М. Использование элементов математической статистики, теории линейных рекуррентных последовательностей и теории булевых функций в криптографии. Владивосток: ДВГУ, 2007.

6. Гончаров С.М. Криптоанализ ручных шифров. Владивосток: ДВГУ, 2007.

7. В.Столлингс. Криптография и защита сетей. М.: изд. Дом «Вильямс», 2002.

8. Н.Смарт. Криптография. М.: «Техносфера», 2005.

9. Фомичев В.М. Дискретная математика и криптология. М.: ДИАЛОГ-МИФИ, 2003.

10. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. СПб.: НПО "Профессионал", 2004.

11. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В.. Математические и компьютерные основы криптологии. Минск: «Новое знание», 2003

12. Bruce Schneier Applied Cryptography: protocols, algorithms and source codes in C. John Wiley & Sons, Inc. 1994.

13. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone Handbook of Applied Cryptography. CRC Press, 1996.

Методическое обеспечение:

1. С.М Гончаров. Использование элементов математической статистики, теории линейных рекуррентных последовательностей и теории булевых функций в криптографии. Методические указания к выполнению практических заданий. - Владивосток: Изд-во ДВГУ, 2007.
2. С.М Гончаров. Криптоанализ ручных шифров. Методические указания к выполнению лабораторного практикума. - Владивосток: Изд-во ДВГУ, 2007.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Дальневосточный федеральный университет»

(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Криптографические методы защиты информации»

Специальность 10.05.01 Компьютерная безопасность

специализация «Математические методы защиты информации»

Форма подготовки очная

Владивосток

2019

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-4) способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знает	методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
	Умеет	применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
	Владеет	методикой и методологией научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
(ОПК-10) способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Знает	современные языки программирования и программные комплексы
	Умеет	строить алгоритмы
	Владеет	способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Введение в криптографию	ОПК-4 ОПК-10	знает	собеседование (ОУ-1)	1-7
			умеет	коллоквиум (ОУ-2)	1-7
			владеет	конспект (ПР-7)	1-7
2	Раздел II. Основные классы шифров и их свойства	ОПК-4 ОПК-10	знает	собеседование (ОУ-1)	8-10
			умеет	коллоквиум (ОУ-2)	8-10
			владеет	конспект (ПР-7)	8-10
3	Раздел III.	ОПК-4 ОПК-10	знает	собеседование (ОУ-1)	11-19

	Надежность шифров		умеет	коллоквиум (ОУ-2)	11-19
			владеет	конспект (ПР-7)	11-19
4	Раздел VI. Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии	ОПК-4 ОПК-10	знает	собеседование (ОУ-1)	20-25
			умеет	коллоквиум (ОУ-2)	20-25
			владеет	конспект (ПР-7)	20-25
5	Раздел V. Современные системы	ОПК-4 ОПК-10	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	
6	Раздел VI. Общие вопросы	ОПК-4 ОПК-10	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
(ОПК-4) способность применять методологию научных исследований в	Знает	методологию научных исследований в профессиональной деятельности, в том числе в	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы;

профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами		работе над междисциплинарными и инновационными проектами		ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	Умеет	применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно строить модели простых неформализуемых задач самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	Владеет	методикой и методологией научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно создать вычислительную сеть для решения прикладных инженерных задач.
(ОПК-10) способностью к самостоятельн	Знает	современные языки программирования и	полнота и системность знаний	изложение полученных знаний полное, в соответствии

ому построению алгоритма, проведению его анализа и реализации в современных программных комплексах		программные комплексы		с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	Умеет	строить алгоритмы	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно строить модели простых неформализуемых задач самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	Владеет	способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно создать вычислительную сеть для решения прикладных инженерных задач.

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Введение в криптографию	ОПК-4	знает	Практическое задание (ПР-7)	1-7
			умеет	Практическое задание (ПР-7)	1-7
			владеет	Практическое задание (ПР-7)	1-7
2	Раздел II. Основные классы шифров и их свойства	ОПК-4	знает	Практическое задание (ПР-7)	8-10
			умеет	Практическое задание (ПР-7)	8-10
			владеет	Практическое задание (ПР-7)	8-10
3	Раздел III. Надежность шифров	ОПК-4	знает	Практическое задание (ПР-7)	11-19
			умеет	Практическое задание (ПР-7)	11-19
			владеет	Практическое задание (ПР-7)	11-19
4	Раздел VI. Методы математической статистики, теории булевых функций и теории	ОПК-10	знает	Практическое задание (ПР-7)	20-25
			умеет	Практическое задание (ПР-7)	20-25
			владеет	Практическое задание (ПР-7)	20-25

	линейных рекуррентных последовательностей в криптографии				
5	Раздел V. Современные системы	ОПК-10	знает	Практическое задание (ПР-7)	
			умеет	Практическое задание (ПР-7)	
			владеет	Практическое задание (ПР-7)	
6	Раздел VI. Общие вопросы	ОПК-10	знает	Практическое задание (ПР-7)	
			умеет	Практическое задание (ПР-7)	
			владеет	Практическое задание (ПР-7)	

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

В 7 семестре экзамен выставляется на основании сдачи всех самостоятельных работ и сдачи экзаменационного билета.

Для подготовки к ответу на экзамене обучающийся получает 20 минут. В ходе подготовки обучающийся может составлять любые записи, однако оценивается прежде всего устный, а не письменный ответ.

При определении оценки ответа обучающегося как на экзамене, так и на практическом занятии учитываются:

- соблюдение норм литературной речи;
- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.

Для получения «зачтено» ответ студента должен соответствовать следующим минимальным требованиям: полный ответ на 1 вопрос или частичный ответ на 2 вопроса; допускаются нарушения в последовательности изложения; демонстрируются поверхностные знания вопроса; имеются затруднения с выводами; допускаются нарушения норм литературной речи.

Оценка **«не зачтено»** выставляется в случае, если: обучающийся не ответил полно ни на один вопрос; материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине; имеются заметные нарушения норм литературной речи.

Оценочные средства для промежуточной аттестации
Список вопросов на экзамен

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 Маркова

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 A5. Шифрсистема Гиффорда. Фильтрующие генераторы. Комбинирующие генераторы

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

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются конспект (ПР-7).

Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание конспекта
Отлично	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы, а также содержит сведения из дополнительных источников.
Хорошо	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Удовлетворительно	Конспект содержит базовые понятия, термины, положения, изученные на лекции.
Неудовлетворительно	Конспект не содержит основных понятий, терминов, положений по данной теме.