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

Направление подготовки 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. 18 /лаб. 00 час.
в том числе в электронной форме лек. 00 /пр. 00 /лаб. 00 час.
всего часов аудиторной нагрузки 144 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 45 час.
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: Власов А.А.

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)

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.27.

Общая трудоемкость дисциплины 216 часов (6 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), практические занятия (108 час.), самостоятельная работа (72 час., в том числе 45 час. на подготовку к экзамену). Дисциплина реализуется на 4 курсе в 7 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Криптографические методы защиты информации» логически и содержательно связана с такими курсами, как «Математический анализ», «Основы геометрии», «Основы алгебры в криптологии».

Содержание дисциплины охватывает следующий круг вопросов: фундаментальные знания теории функции комплексного числа, множества на комплексной плоскости, основные элементарные функции комплексного переменного, многозначные функции.

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;
- изучить принципов синтеза и анализа шифров;
- ознакомить 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).

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	навыком самостоятельного построения алгоритма, проведения его анализа и реализацией 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: конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2).

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 (6 час.)

Тема 1. Теория К. Шеннона (2 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 (2 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 IV. Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии (6 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 (2 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 (2 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 (21 час.)

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

Занятие 2. Модели открытых текстов. Избыточность языка (21 час.)

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

Занятие 3. Вскрытие шифров замены с использованием статистических закономерностей открытых сообщений (22 час.)

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

Занятие 4. Вскрытие шифров перестановки (22 час.)

1. Методы перестановки.
2. Использование шифров перестановки.
3. Вскрытие шифров перестановки.

Занятие 5. Определение короткой гаммы по шифротексту (22 час.)

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

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	ПР-7	1-6
			умеет	ОУ-1	1-6
			владеет	ОУ-2	1-6
2	Раздел II. Основные классы шифров и их свойства	ОПК-4, ОПК-10	знает	ПР-7	7-9
			умеет	ОУ-1	7-9
			владеет	ОУ-2	7-9
3	Раздел III. Надежность шифров	ОПК-4, ОПК-10	знает	ПР-7	10-12
			умеет	ОУ-1	10-12
			владеет	ОУ-2	10-12
4	Раздел IV. Методы математической статистики, теории булевых функций и теории линейных рекуррентных последовательностей в криптографии	ОПК-4, ОПК-10	знает	ПР-7	13-15
			умеет	ОУ-1	13-15
			владеет	ОУ-2	13-15
5	Раздел V. Современные системы	ОПК-4, ОПК-10	знает	ПР-7	16-18
			умеет	ОУ-1	16-18
			владеет	ОУ-2	16-18
6	Раздел VI. Общие вопросы	ОПК-4, ОПК-10	знает	ПР-7	19-22
			умеет	ОУ-1	19-22
			владеет	ОУ-2	19-22

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

(электронные и печатные издания)

1. Орлов В.А. Теория чисел в криптографии: учебное пособие / В.А. Орлов, Н.В. Медведев, Н.А. Шимко, А.Б. Домрачева — 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: монография / Б.Я. Рябко, А.Н. Фионов — Москва : Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192

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

Дополнительная литература

(электронные и печатные издания)

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

2. Боровков, А.А. Математическая статистика: учебник / А.А. Боровков — Санкт-Петербург : Лань, 2010. — 704 с. — Режим доступа: https://e.lanbook.com/book/3810

3. Кукина, Е.Г. Введение в криптографию: сборник задач и упражнений / Е.Г. Кукина, В.А. Романьков — Омск : ОмГУ, 2013. — 91 с. — Режим доступа: https://e.lanbook.com/book/75394

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Механизмы защиты информации [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.intuit.ru/studies/courses/16655/1300/lecture/25505?page=2
2. Криптографические методы защиты информации [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://sec4all.net/modules/myarticles/article.php?storyid=605
3. Криптографические методы защиты информации [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://studfiles.net/preview/5201682/page:9/

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 608, 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 лот 4. 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 144 часа. На самостоятельную работу – 72 часа, в том числе 45 часов на подготовку к экзамену. 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 – экзамен. Вопросы к экзамену соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к экзамену 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 L, ауд. L 608, 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 – 30) Оборудование: 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 профессионального образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Криптографические методы защиты информации»
Направление подготовки 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
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 недели обучения	Подготовка практического задания (выполнение отчетов к практическим работам № 1-5)	27	Отчеты о выполнении
2	Сессия	Подготовка к экзамену	45	Экзамен

Подготовка отчета по практическим работам предполагает повторение лекционного материала и выполнение задания для практических работ по темам из Раздела II РПУД.

В ходе самостоятельной работы обучающийся должен подготовить для сдачи отчёт по проделанной работе. Необходимо указать в отчёте следующую информацию: название и цель работы, краткий теоретический материал, задание на практическую работу, ход работы, полученные результаты и выводы. По результатам защиты отчёта студенту выставляется «зачтено» или «не зачтено». Студент получает «зачтено», если отчёт содержит все перечисленные ранее пункты и оформлен в соответствии с правилами оформления письменных работ.

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, а также основной и дополнительной литературы из списка рекомендуемых источников. Список вопросов для подготовки к экзамену, а также методические рекомендации по оцениванию представлены в Приложении 2 РПУД

Приложение 2

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

ШКОЛА ЕСТЕССТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Криптографические методы защиты информации»
Направление подготовки 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Шкала оценивания уровня сформированности 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	навыком самостоятельного построения алгоритма, проведения его анализа и реализацией 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	ПР-7	1-6
			умеет	ОУ-1	1-6
			владеет	ОУ-2	1-6
2	Раздел II. Основные классы шифров и их свойства	ОПК-4, ОПК-10	знает	ПР-7	7-9
			умеет	ОУ-1	7-9
			владеет	ОУ-2	7-9
3	Раздел III. Надежность шифров	ОПК-4, ОПК-10	знает	ПР-7	10-12
			умеет	ОУ-1	10-12
			владеет	ОУ-2	10-12
4	Раздел IV. Методы математической статистики, теории	ОПК-4, ОПК-10	знает	ПР-7	13-15
			умеет	ОУ-1	13-15
			владеет	ОУ-2	13-15

	булевых функций и теории линейных рекуррентных последовательностей в криптографии				
5	Раздел V. Современные системы	ОПК-4, ОПК-10	знает	ПР-7	16-18
			умеет	ОУ-1	16-18
			владеет	ОУ-2	16-18
6	Раздел VI. Общие вопросы	ОПК-4, ОПК-10	знает	ПР-7	19-22
			умеет	ОУ-1	19-22
			владеет	ОУ-2	19-22

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине - экзамен.

Для допуска к экзамену необходимо сдать все практические задания. В случае, если ко дню проведения экзамена обучающийся не сдал какие-либо из практических заданий, он получает возможность сдать их на консультации перед экзаменом. Экзамен выставляется на основании сдачи всех практических заданий и сдачи экзаменационного билета.

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.

Оценочные средства для промежуточной аттестации

Список вопросов на экзамен

1. Основные методы защиты информации.
2. Исторические примеры: шифр Цезаря, квадрат Полибия, шифр Виженера, шифр Сцитала, решетка Кардано, книжный шифр и др.
3. Основные этапы становления криптографии как науки.

4. Открытые сообщения и их характеристики.

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

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

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

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

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

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

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

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

13. Методы матстатистики в криптографии.

14. Специальные вопросы теории двоичных функций.

15. Элементы теории ЛРП, используемые в криптографии.

16. Блочное шифрование.

17. Поточные системы шифрования.

18. Методы анализа криптографических алгоритмов.

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

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

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

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

Каждый экзаменационный билет содержит два вопроса из списка выше. Результаты экзамена оцениваются по четырёхбалльной системе («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») и заносятся в экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки.

При определении оценки учитываются:

- 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, сведениям из информационных ресурсов Интернет.

Оценка **«отлично».** Ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания дисциплины. Соблюдаются нормы литературной речи.

Оценка **«хорошо».** Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.

Оценка **«удовлетворительно».** Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.

Оценка **«неудовлетворительно».** Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи.

В случае неявки студента на экзамен в экзаменационной ведомости делается отметка «не явился».

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются конспект (ПР-7) и лабораторные работы (ПР-6).

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.

Для оценки продвинутого и высокого уровня сформированности компетенции проводятся лабораторные работы. Темы практических работ представлены в Разделе II РПУД. Критерии оценки представлены в таблице:

Оценка	Критерий
Зачтено	Отчёт по практической работе содержит все необходимые пункты (цель работы, краткий теоретический материал, задание на практическую работу, ход работы, полученные результаты, выводы). Оформление отчёта соответствует правилам оформления письменных работ. Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Незачтено	Отчёт по практической работе не содержит какого-либо необходимого пункта(ов) и/или оформление отчёта не соответствует правилам оформления письменных работ. Конспект не содержит основных понятий, терминов, положений по данной теме