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
Теория псевдослучайных генераторов
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс 4 семестр 8
лекции 36 час.
практические занятия 54 час.
лабораторные работы 18 час.
в том числе с использованием МАО лек. 9 / пр. 36 / лаб. 00 час.
в том числе в электронной форме лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 90 час.
в том числе с использованием МАО 45 час.
в том числе в электронной форме 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 8 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 (ли): Корнюшин П.Н. д.ф.-м.н., профессор

Владивосток
2019

I. 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: *Theory of pseudo-random generators*

Basic part of Block 1, _5_credits

Instructor: *Kornyushin P.N.*

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

• *ability to correctly apply 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) when solving professional problems;*

• *ability to apply research methods in professional activities, including in the work on interdisciplinary and innovative projects (OPK-4);*

• *ability to use programming languages and systems, tools for solving professional, research and applied tasks (OPK-8).*

Learning outcomes:

(PSK-2.1) the ability to develop computational algorithms that implement modern mathematical methods for protecting information

(CPM-2.2) the ability, based on the analysis of the applied mathematical methods and algorithms, to evaluate the effectiveness of information protection means and methods in computer systems

(CPM-2.4) the ability to develop, analyze and justify the adequacy of mathematical models of the processes arising from the operation of software and hardware information protection.

Course description:

Discipline has a theoretical orientation, with great importance for the development of the discipline are both lectures and laboratory and practical classes. During the implementation of the discipline in the framework of lectures, laboratory and practical classes, methods of active / interactive learning are used

that implement a visual presentation of the results of the pseudo-random number generator algorithm. The discipline "Theory of Pseudo-Random Generators" provides for the acquisition of knowledge and skills in the field of the pseudo-random number generator algorithm, generating a sequence of numbers whose elements obey a given distribution. The study of this discipline contributes to the development of the principles of the use of a pseudo-random number generator in computer science - from the Monte-Carlo method and simulation to cryptography.

Main course literature:

1. Нерсесянц А.А. Защита информации [Электронный ресурс] : учебное пособие / А.А. Нерсесянц. — Электрон. текстовые данные. — Ростов-на-Дону: Северо-Кавказский филиал Московского технического университета связи и информатики, 2010. — 61 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61295.html

2. Аверченков В.И. Организационная защита информации [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 184 с. — 978-89838-489-0. — Режим доступа: http://www.iprbookshop.ru/7002.html

3. Каторин Ю.Ф. Защита информации техническими средствами [Электронный ресурс] : учебное пособие / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2012. — 417 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66445.html

Form of final control: *exam*

Аннотация к рабочей программе дисциплины «Теория псевдослучайных генераторов»

Рабочая программа дисциплины «Теория псевдослучайных генераторов» разработана для студентов 4 курса специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в базовую часть дисциплин учебного плана Б1.Б.40.2.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единицы, 180 часа. Учебным планом предусмотрены лекционные занятия (36 часов), лабораторные работы (18 часов), практические занятия (54 часов),

самостоятельная работа (72 час, в том числе 45 час на подготовку к экзамену). Дисциплина реализуется на 4 курсе, в 8 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Теория псевдослучайных генераторов» основана на предварительном изучении следующих дисциплин: «Математическая логика и теория алгоритмов», «Алгебра», «Языки программирования».

Дисциплина имеет теоретическую направленность, при этом большое значение для освоения дисциплины имеют как лекционные занятия, так и лабораторные и практические занятия. В ходе реализации дисциплины в рамках лекционных, лабораторных и практических занятий применяются методы активного/ интерактивного обучения, реализующие наглядное представление результатов алгоритма генератора псевдослучайных чисел. Дисциплина «Теория псевдослучайных генераторов» обеспечивает приобретение знаний и умений в области алгоритма генератора псевдослучайных чисел, порождающего последовательность чисел, элементы которой подчиняются заданному распределению. Изучение этой дисциплины способствует освоению принципов применения генератора псевдослучайных чисел в информатике – от метода Монте-Карло и имитационного моделирования до криптографии.

Цель - подготовка к научно-исследовательской деятельности в областях, использующих математические методы и компьютерные технологии; подготовка к работе, связанной с решением различных задач, предполагающих использование математического моделирования процессов и объектов и программного обеспечения; подготовка к работе в сфере защиты информации.

Задачи:

- изучить основные определения и понятия теории псевдослучайных генераторов;
- изучить основные способы построения псевдослучайных генераторов;

- разрабатывать и анализировать математические модели процессов с использованием генератора псевдослучайных чисел.

Для успешного изучения дисциплины «Теория псевдослучайных генераторов» 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 применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами(ОПК-4);
- способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8).

В результате изучения данной дисциплины у обучающихся формируются следующие профильно-специализированные компетенции:

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ПСК-2.1) способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает	Принципы построения и свойства псевдослучайных генераторов
	Умеет	Составлять конспект по изучаемому материалу, делать выводы в ходе выполнения практических заданий.
	Владеет	Основными знаниями в области теории псевдослучайных генераторов
(ПСК-2.2) способностью на основе анализа применяемых	Знает	Основные определения и понятия теории псевдослучайных генераторов

математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Умеет	Формулировать результат проведенных исследований в ходе выполнения практических заданий.
	Владеет	Основными терминами предметной области.
(ПСК-2.4) способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знает	Основные способы построения псевдослучайных генераторов
	Умеет	Научно и практически обосновано излагать результаты исследований
	Владеет	Основными знаниями в построении псевдослучайных генераторов

Для формирования вышеуказанных компетенций в рамках дисциплины «Теория псевдослучайных генераторов» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: конспекты (ПР-7), лабораторные работы (ПР-6), собеседование (ОУ-1), коллоквиум (ОУ-2).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Принципы построения и свойства псевдослучайных генераторов (12 час.)

Тема 1. Задачи, для которых используются псевдослучайные генераторы (ПСГ) Принципы построения ПСГ**(2 час.)**

Тема 2. Криптографические требования к стойкости ПСГ Статистические требования к стойкости ПСГ. Классификация ПСГ**(2 час.)**

Тема 3. Поле. Примитивный многочлен. Генератор ненулевых элементов поля. **(2 час.)**

Тема 4. Реализация генераторов ненулевых элементов поля. Примеры. **(2 час.)**

Тема 5. Устройства функционирующие в GF(L). **(2 час.)**

Тема 6. Свойства генераторов М-последовательностей. **(2 час.)**

Раздел II. Стохастические генераторы псевдослучайных последовательностей (10 час.)

Тема 1. Алгоритм работы стохастического генератора. Двухступенчатые стохастические генераторы многоразрядных ПСП. **(2 час.)**

Тема 2. Принципы адресации в R-блоке. Основные проблемы стохастических генераторов. **(2 час.)**

Тема 3. Графические тесты. Гистограмма распределения элементов. Распределение на плоскости. **(2 час.)**

Тема 4. Графические тесты. Проверка серий. Проверка на монотонность. **(2 час.)**

Тема 5. Графические тесты. Битовая автокорреляционная функция. Символьная автокорреляционная функция. **(2 час.)**

Раздел III. Поточные шифры (14 час.)

Тема 1. Поточный шифр**(2 час.)**

Тема 2. Синхронные поточные шифры**(2 час.)**

Тема 3. Самосинхронизирующиеся поточные шифры**(2 час.)**

Тема 4. Метод "Одноразовых блокнотов"**(2 час.)**

Тема 5. Элементная база криптосхем**(2 час.)**

Тема 6. Комбинирующие генераторы**(2 час.)**

Тема 7. Генераторы с перемежающимся шагом**(2 час.)**

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (54 час.)

Занятие 1. Конгруэнтные генераторы (8 час.)

Занятие 2. Алгоритм Берлекемпа-Месси (10 час.)

Занятие 3. Генератор на основе Вихря Мерсенна (8 час.)

Занятие 4. Исследование выходных последовательностей (10 час.)

Занятие 5. Исследование методов оценки качества (6 час.)

Занятие 6. Реализация криптографического генератора псевдослучайных последовательностей (12 час.)

Лабораторные работы (18 час.)

Лабораторная работа № 1. Генераторы ПСП. (10 час.)

Лабораторная работа № 2. Поточные шифры. (8 час.)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Теория псевдослучайных генераторов» 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 - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Принципы построения и свойства псевдослучайных генераторов	ПСК-2.1, ПСК-2.2, ПСК-2.4	знает	УО-2	1-20
			умеет	УО-2	1-20
			владеет	УО-2	1-20
2	Раздел II Стохастические генераторы псевдослучайных последовательностей	ПСК-2.1, ПСК-2.2, ПСК-2.4	знает	ПР-6	20-26
			умеет	ПР-6	20-26
			владеет	ПР-6	20-26
3	Раздел III. Поточные шифры	ПСК-2.1, ПСК-2.2, ПСК-2.4	знает	ПР-6	30-38
			умеет	ПР-6	30-38
			владеет	ПР-6	30-38

Задачи для практических занятий по Модулю 1 «Введение в дискретную теорию информации и кодирование» соответствуют задачам по соответствующим разделам из учебного пособия.

Практические задания и контрольные вопросы по Модулю 2 «Основы корректирующего кодирования» соответствуют заданиям по соответствующим темам из учебного пособия.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Нерсесянц А.А. Защита информации [Электронный ресурс] : учебное пособие / А.А. Нерсесянц. — Электрон. текстовые данные. — Ростов-на-

Дону: Северо-Кавказский филиал Московского технического университета связи и информатики, 2010. — 61 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61295.html
2. Аверченков В.И. Организационная защита информации [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 184 с. — 978-89838-489-0. — Режим доступа: http://www.iprbookshop.ru/7002.html
3. Каторин Ю.Ф. Защита информации техническими средствами [Электронный ресурс] : учебное пособие / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2012. — 417 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66445.html

Дополнительная литература

(печатные и электронные издания)

1. Гатченко Н.А. Криптографическая защита информации [Электронный ресурс] / Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2012. — 142 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/68658.html
2. Каторин Ю.Ф. Техническая защита информации [Электронный ресурс] : лабораторный практикум / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2013. — 113 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/68715.html
3. Титов А.А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие / А.А. Титов. — Электрон. текстовые данные. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/13931.html

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Теория псевдослучайных генераторов», составляет 90 часов. На самостоятельную работу – 27 часа. При этом аудиторная нагрузка состоит из 36 лекционных часов и 54 часов практических занятий.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Подготовка к практическим занятиям предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии. Основной практической составляющей является выполнение одного практического задания с последующим предоставлением отчета о выполнении.

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

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 654(752), 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 – 90) Оборудование: "Мультимедийное оборудование: Экран проекционный Projecta Elpro Large Electron, 500x316 см, размер рабочей области 490x306 Документ-камера Avervision CP 355 AF Мультимедийный проектор Panasonic PT-DZ11OXE, 10 600 ANSI Lumen, 1920x1200 Сетевая видеокамера Multipix MP-HD718 ЖК-панель 47"", Full HD, LG M4716

	ССВА ЖК-панель 42"", Full HD, LG M4214 ССВА ЖК-панель 42"", Full HD, LG M4214 ССВА" Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 549а, Компьютерный класс, 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 – 15) Оборудование: Компьютер (твердотельный диск - объемом 128 ГБ; жесткий диск - объем 1000 ГБ; форм-фактор - Tower; комплектуется клавиатурой, мышью, монитором AOC i2757Fm; комплектом шнуров эл. питания) модель - M93p 1 Доска аудиторная

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 «Теория псевдослучайных генераторов»

Направление подготовки 10.05.01 Компьютерная безопасность

специализация «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 неделя обучения	Подготовка практического задания (выполнение отчета к занятию)	27	Отчет о выполнении практического задания
2	Сессия	Подготовка и сдача экзамена	45	Экзамен

Рекомендации по самостоятельной работе студентов

При подготовке отчета о выполнении практического задания должны использоваться источники из списка учебной литературы, а также примеры, рассмотренные на лекционных и практических занятиях. Отчет должен содержать:

- титульный лист;
- содержание;
- описание задания;
- решение;
- выводы.

Методические указания к выполнению отчета по занятию

Для получения **«зачтено»** отчет должен содержать основные пункты: титульный лист, содержание, описание задания, решение, выводы. При представлении отчета к сдаче обучающийся последовательно излагает принцип выполненной работы.

Оценка **«незачтено»** выставляется в случае, если отчет не содержит решения или выводов; обучающийся не может объяснить решение, излагает материал непоследовательно, сбивчиво.

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 «Теория псевдослучайных генераторов»
Направление подготовки 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
(ПСК-2.1) способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает	Принципы построения и свойства псевдослучайных генераторов
	Умеет	Составлять конспект по изучаемому материалу, делать выводы в ходе выполнения практических заданий.
	Владеет	Основными знаниями в области теории псевдослучайных генераторов
(ПСК-2.2) способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знает	Основные определения и понятия теории псевдослучайных генераторов
	Умеет	Формулировать результат проведенных исследований в ходе выполнения практических заданий.
	Владеет	Основными терминами предметной области.
(ПСК-2.4) способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знает	Основные способы построения псевдослучайных генераторов
	Умеет	Научно и практически обосновано излагать результаты исследований
	Владеет	Основными знаниями в построении псевдослучайных генераторов

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Принципы построения и свойства псевдослучайных генераторов	ПСК-2.1, ПСК-2.2, ПСК-2.4	знает	УО-2	1-20
			умеет	УО-2	1-20
			владеет	УО-2	1-20

2	Раздел II Стохастические генераторы псевдослучайных последовательностей	ПСК-2.1, ПСК-2.2, ПСК-2.4	знает	ПР-6	20-26
			умеет	ПР-6	20-26
			владеет	ПР-6	20-26
3	Раздел III. Поточные шифры	ПСК-2.1, ПСК-2.2, ПСК-2.4	знает	ПР-6	30-38
			умеет	ПР-6	30-38
			владеет	ПР-6	30-38

Оценочные средства для промежуточной аттестации

Список вопросов на экзамен

1. Задачи, для которых используются псевдослучайные генераторы (ПСГ)
2. Принципы построения ПСГ
3. Криптографические требования к стойкости ПСГ
4. Статистические требования к стойкости ПСГ
5. Классификация ПСГ
6. BBS-генератор
7. RSA-генератор
8. Линейный конгруэнтный генератор
9. Полиномиальный конгруэнтный генератор
10. Аддитивный генератор Фибоначчи. Аддитивный генератор Фибоначчи с запаздыванием
11. Мультипликативный генератор Фибоначчи с запаздыванием
12. Инверсивный конгруэнтный генератор
13. LFSR-генераторы. Достоинства, недостатки и области применения.
14. LFSR-генераторы. Образующий многочлен. Примеры генераторов Галуа и Фибоначчи
15. Генератор двоичных последовательностей. Сопровождающая матрица.
16. М-последовательность. Генератор М-последовательности. Характеристический многочлен
17. Связь между образующим и характеристическим многочленом
18. Децимация последовательности

19. Функции усложнения. NLFSR-генераторы. Генератор Джиффи. Генератор Голлманна. Аддитивный генератор
20. Структурная схема ПСГ
21. Поле. Примитивный многочлен. Генератор ненулевых элементов поля.
22. Реализация генераторов ненулевых элементов поля. Примеры.
23. Устройства функционирующие в GF(L).
24. Свойства генераторов М-последовательностей.
25. ЛРП. Характеристический многочлен ЛРП. Период ЛРП. Аннулятор ЛРП.
26. Алгоритм Берлекмпа-Месси
27. Алгоритм работы стохастического генератора.
28. R-блок.
29. Принципы адресации в R-блоке.
30. Стохастические генераторы на регистрах сдвига (RFSR).
31. Криптоанализ RFSR.
32. Двухступенчатые стохастические генераторы многоразрядных ПСП.
33. Стохастические генераторы ПСП с многораундовой функцией обратной связи.
34. Основные проблемы стохастических генераторов.
35. Графические тесты. Гистограмма распределения элементов. Распределение на плоскости.
36. Графические тесты. Проверка серий. Проверка на монотонность.
37. Графические тесты. Битовая автокорреляционная функция. Символьная автокорреляционная функция.
38. Графические тесты. Профиль линейной сложности. Графический спектральный тест.

Критерии выставления оценки на экзамене

Оценка	Требования к сформированным компетенциям
«отлично»	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, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач по методологии научных исследований.
«хорошо»	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, владеет необходимыми навыками и приемами их выполнения.
«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства для текущей аттестации

№ п/п	Код ОС	Наименование оценочного средства	Кроткая характеристика оценочного средства	Представление оценочного средства в фонде
1	ОУ-1	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы,	Вопросы по темам/разделам дисциплины

			связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п.	
2	ОУ-2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
3	ПР-6	Лабораторная работа	Средство для закрепления и практического освоения материала по определенному разделу	Комплект лабораторных заданий
4	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины