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.
всего часов аудиторной нагрузки 108 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 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): Боршевников А.Е., ассистент штатный

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: *theory of pseudo-random generators*

Basic part of Block 1, _5_credits.

Instructor: Borshevnikov A.E.

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

- the ability to correctly apply in solving professional problems apparatus of mathematical analysis, geometry, algebra, discrete mathematics, mathematical logic, theory of algorithms, probability theory, mathematical statistics, information theory, number-theoretic methods (OPK-2).

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 security tools

Course description: 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»

Курс учебной дисциплины «Теория псевдослучайных генераторов» предназначен для обучения студентов направления 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин базовой части учебного плана Б1.Б.7

Общая трудоемкость освоения дисциплины составляет 180 часов (5 з.е.). Учебным планом предусмотрены лекционные занятия (36 часа), лабораторные работы (18 часов), практические занятия (54 часов), самостоятельная работа (27 часов, в том числе 45 часов на подготовку к экзамену). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Теория псевдослучайных генераторов» логически и содержательно связана с такими дисциплинами, как «Математическая логика и теория алгоритмов», «Алгебра», «Теория вероятностей и математическая статистика».

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 изучения дисциплины «Теория псевдослучайных генераторов» заключается в подготовке 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).

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

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	Знает	методы анализа и обоснования

основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах		адекватности математических процессов, возникающих при работе программно-аппаратных средств защиты информации.
	Умеет	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
	Владеет	способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.
(ПСК-2.4) способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знает	методы анализа и обоснования адекватности математических процессов, возникающих при работе программно-аппаратных средств защиты информации.
	Умеет	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
	Владеет	способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.

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: конспект (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 (12 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. **(4 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 (12 час.)

Тема 1. Поточный шифр**(2 час.)**

Тема 2. Синхронные поточные шифры**(4 час.)**

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

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

Тема 5. 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 (8 час.)

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

Занятие 4. Исследование выходных последовательностей (10 час.)

Занятие 5. Исследование методов оценки качества (10 час.)

Занятие 6. Реализация криптографического генератора псевдослучайных последовательностей (10 час.)

Лабораторные работы (18 час.)

Лабораторная работа № 1. Генераторы ПСП. (9 час.)

Лабораторная работа № 2. Поточные шифры. (9 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	собеседование (ОУ-1) коллоквиум (ОУ-2)	1-20
			умеет	лабораторные работы (ПР-6),	1-20
			владеет	конспект (ПР-7)	1-20
2	Раздел II Стохастические генераторы псевдослучайных последовательностей	ПСК-2.1 ПСК-2.2 ПСК-2.4	знает	собеседование (ОУ-1) коллоквиум (ОУ-2)	20-26
			умеет	лабораторные работы (ПР-6),	20-26
			владеет	конспект (ПР-7)	20-26
3	Раздел III. Поточные шифры	ПСК-2.1 ПСК-2.2 ПСК-2.4	знает	собеседование (ОУ-1) коллоквиум (ОУ-2)	30-38
			умеет	лабораторные работы (ПР-6),	30-38
			владеет	конспект (ПР-7)	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. Русанов В.Э., Лобов Е.М. Построение и исследование схем дискретной логики, используемых при создании помехоустойчивых кодеков (схемы умножения и деления полиномов, а также генератора псевдослучайных последовательностей) [Электронный ресурс]: практикум № 5 ПК/ — Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2014.— 15 с.— Режим доступа: http://www.iprbookshop.ru/63348.html

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 547, 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 «Теория псевдослучайных генераторов», составляет 96 часов. На самостоятельную работу – 84 часа. При этом аудиторная нагрузка состоит из 32 лекционных часа и 48 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 547, 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 – 26) 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 «Теория псевдослучайных генераторов»

Специальность 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 заданию 1)	27	Отчет о выполнении
2	Сессия	Подготовка к экзамену	45	Экзамен

Подготовка отчета к практическому заданию предполагает повторение лекционного материала и выполнение практического задания. В результате студент должен предоставить отчет о проделанной работе.

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

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»
Специальность 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	методы анализа и обоснования адекватности математических процессов, возникающих при работе программно-аппаратных средств защиты информации.
	Умеет	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
	Владеет	способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.
(ПСК-2.4) способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знает	методы анализа и обоснования адекватности математических процессов, возникающих при работе программно-аппаратных средств защиты информации.
	Умеет	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
	Владеет	способностью разрабатывать, анализировать и обосновывать

		адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.

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	собеседование (ОУ-1) коллоквиум (ОУ-2)	1-20
			умеет	лабораторные работы (ПР-6),	1-20
			владеет	конспект (ПР-7)	1-20
2	Раздел II Стохастические генераторы псевдослучайных последовательностей	ПСК-2.1 ПСК-2.2 ПСК-2.4	знает	собеседование (ОУ-1) коллоквиум (ОУ-2)	20-26
			умеет	лабораторные работы (ПР-6),	20-26
			владеет	конспект (ПР-7)	20-26
3	Раздел III. Поточные шифры	ПСК-2.1 ПСК-2.2 ПСК-2.4	знает	собеседование (ОУ-1) коллоквиум (ОУ-2)	30-38
			умеет	лабораторные работы (ПР-6),	30-38
			владеет	конспект (ПР-7)	30-38

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
(ПСК-2.1) способностью разрабатывать вычислительные алгоритмы,	Знает (пороговый уровень)		Полнота с системность знаний.	стандартные алгоритмы применяемых методов.
	Умеет		Степень	проводить

реализующие современные математические методы защиты информации	(продвинутый)		самостоятельности.	научные эксперименты, обрабатывать результаты эксперимента.
	Владеет (высокий)		Степень владения.	владеть компьютерными пакетами для проведения исследовательских экспериментов.
(ПСК-2.3) способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает(пороговый уровень)		Полнота с системность знаний.	методы анализа и обоснования адекватности математических процессов
	Умеет(продвинутый)		Степень самостоятельности.	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
	Владеет (высокий)		Степень владения.	способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
(ПСК-2.4)	Знает(пороговый уровень)		Полнота с системность	основные алгоритмы

способностью моделировать алгоритмы в системах компьютерной математики, оценивать их работоспособность и эффективность			знаний.	эллиптической криптографии
	Умеет(продвинутый)		Степень самостоятельности.	моделировать алгоритмы в системах компьютерной математики, оценивать эффективность
	Владеет (высокий)		Степень владения.	способностью моделировать алгоритмы.

(ПСК-2.6) способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знает(пороговый уровень)		Полнота с системность знаний.	методы анализа и обоснования адекватности математических процессов
	Умеет(продвинутый)		Степень самостоятельности.	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
	Владеет (высокий)		Степень владения.	способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.

(ПСК-2.7) способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации	Знает(пороговый уровень)		Полнота с системность знаний.	основные алгоритмы эллиптической криптографии
	Умеет(продвинутый)		Степень самостоятельности.	моделировать алгоритмы в системах компьютерной математики, оценивать эффективность

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Заполняется в соответствии с Положением о фондах оценочных средств образовательных программ высшего образования – программ бакалавриата, специалитета, магистратуры ДВФУ, утвержденным приказом ректора от 12.05.2015 №12-13-850.

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.