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 18 час.
лабораторные работы 18 час.
в том числе с использованием МАО лек. 0 / пр. 0 / лаб. 0 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 36 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: 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)

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, _4_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 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 apply research methods in professional activities, including in the work on interdisciplinary and innovative projects (OPK-4);

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

Learning outcomes:

- (OPK-9) the ability to develop formal models of security policies, access control policies and information flows in computer systems, taking into account information security threats
- (PSK-2.1) the ability to develop computational algorithms that implement modern mathematical methods for protecting information
- (PSK-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 work of software and hardware information protection

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 c. — 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 c. — 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» разработан для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.13.02.

Общая трудоемкость курса 4 зачетные единицы, 144 академических часа. Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (18 час.), практические занятия (18 час.), самостоятельная работа (36 час.), подготовка к экзамену (36 час.). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – экзамен.

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

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 обучающихся к научно-исследовательской деятельности в областях, использующих математические методы и компьютерные технологии, а также 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 общепрофессиональные, профессионально-специализированные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	основные прикладные аспекты псевдослучайных генераторов
	Умеет	разрабатывать формальные модели политик безопасности
	Владеет	навыками разработки формальных моделей политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации

(ПСК-2.1) способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает	основные определения и понятия теории псевдослучайных генераторов
	Умеет	разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации
	Владеет	основными терминами предметной области
(ПСК-2.2) способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знает	основные способы построения псевдослучайных генераторов
	Умеет	оценивать эффективность средств и методов защиты информации в компьютерных системах
	Владеет	способностью анализировать применяемые математические методы и алгоритмы
(ПСК-2.4) способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знает	принципы построения и свойства псевдослучайных генераторов
	Умеет	разрабатывать математические модели процессов
	Владеет	основными знаниями в области теории 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: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Основы теории псевдослучайных генераторов (22 час.)

Тема 1. Принципы построения и свойства псевдослучайных генераторов (4 час.)

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

Тема 2. Генераторы ПСП, функционирующие в конечных полях (9 час.)

1. Поле. Примитивный многочлен. Генератор ненулевых элементов поля.
2. Реализация генераторов ненулевых элементов поля. Примеры.
3. Устройства, функционирующие в GF(L).
4. Свойства генераторов М-последовательностей.

Тема 3. Стохастические генераторы псевдослучайных последовательностей (3 час.)

1. Алгоритм работы стохастического генератора.
2. Принципы адресации в R-блоке.
3. Двухступенчатые стохастические генераторы многоразрядных ПСП.
4. Основные проблемы стохастических генераторов.

Тема 4. Методика оценки качества генераторов псевдослучайных последовательностей (6 час.)

1. Графические тесты. Гистограмма распределения элементов. Распределение на плоскости.
2. Графические тесты. Проверка серий. Проверка на монотонность.
3. Графические тесты. Битовая автокорреляционная функция. Символьная автокорреляционная функция.
4. Графические тесты. Профиль линейной сложности. Графический спектральный тест.
5. Анализ статистической безопасности криптоалгоритмов.

Раздел II. Псевдослучайные генераторы в шифровании и криптографии (14 час.)

Тема 5. Поточные шифры (8 час.)

1. Поточный шифр
2. Синхронные поточные шифры
3. Самосинхронизирующиеся поточные шифры
4. Метод "Одноразовых блокнотов"
5. Криптографические свойства поточных шифров

Тема 6. Криптографические генераторы (6 час.)

1. Элементная база криптосхем
2. Комбинирующие генераторы
3. Генераторы с перемежающимся шагом
4. Каскадные генераторы Голлмана

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (18 час.)

Занятие 1. Конгруэнтные генераторы (3 час.)

1. Реализация полиномиального конгруэнтного генератора
2. Реализация метода распределения точек на плоскости для проверки статистических свойств.

Занятие 2. Алгоритм Берлекемпа-Месси (3 час.)

1. Реализация генератора на основе линейной рекурентной последовательности
2. Реализация алгоритма Берлекемпа-Месси

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

1. Реализация генератора на основе виткового регистра сдвига с обобщенной отдачей "Вихрь Мерсенна"
2. Исследование генератора, разработанного в п.1

Занятие 4. Исследование выходных последовательностей (3 час.)

1. Исследование выходных последовательностей некоторых генераторов псевдослучайных числе на предмет случайности (тест FIPS 140-1)

Занятие 5. Исследование методов оценки качества (3 час.)

1. Исследование методов оценки качества псевдослучайных генераторов

Занятие 6. Реализация криптографического генератора псевдослучайных последовательностей (3 час.)

1. Реализация криптографического генератора псевдослучайных последовательностей.
2. Реализация проверки свойств данного генератора

Лабораторные работы (18 час.)

Лабораторная работа №1. Исследование псевдослучайных последовательностей (2 час.)

Лабораторная работа №2. Реализация генератора (любой из изученных на выбор) (8 час.)

Лабораторная работа №3. Оценка качества псевдослучайных генераторов (2 час.)

Лабораторная работа №4. Криптографический генератор (6 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. Основы теории псевдослучайных генераторов	ОПК-9 ПСК-2.1 ПСК-2.2 ПСК-2.4	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-50
			умеет	лабораторные работы (ПР-6)	1-50
			владеет	конспект (ПР-7),	1-50

				знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	51-69
2	Раздел Псевдослучайные генераторы шифровании криптографии	II. в и	ОПК-9 ПСК-2.1 ПСК-2.2 ПСК-2.4	умеет	лабораторные работы (ПР-6)	51-69
				владеет	конспект (ПР-7),	51-69

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. 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 ресурсов информационно-телекоммуникационной сети «Интернет»

1. https://moluch.ru/archive/142/40025/ Статья «Методы генерации случайных чисел».

2. https://elibrary.ru/ip_restricted.asp?rpage=https%3A%2F%2Felibrary%2Eru%2Fitem%2Easp%3Fid%3D25984330 Генерация случайных и псевдослучайных чисел.

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 733а, Компьютерный класс, 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.
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, 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.

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 734, Компьютерный класс, 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.

Для работы с литературой из списка необходимо наличие у студента аккаунтов в указанных электронно-библиотечных системах: ЭБС «Консультант студента (http://www.studentlibrary.ru), ЭБС «Znanium.com» (http://znanium.com/), ЭБС «IPRBooks» (http://www.iprbookshop.ru/).

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Теория псевдослучайных генераторов», составляет 72 часа. На самостоятельную работу – 36 часов. При этом аудиторная нагрузка состоит

из 36 лекционных часов, 18 часов практических занятий и 18 часов лабораторных работ.

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

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

В рамках указанной дисциплины итоговой формой 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 733а, 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
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, 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: Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk WTL 1810 Мультимедийная аудитория: 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

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 734, 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: "Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Мультимедийное 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

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

(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 к практическим и лабораторным работам	36	Отчет о выполнении
2	Сессия	Подготовка к экзамену	36	Экзамен

Подготовка к лабораторным работам и практическим занятиям предполагает повторение лекционного материала и выполнение задания для лабораторных и 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 лабораторную или 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.

Для допуска к экзамену обучающийся должен получить оценку «зачтено» по всем практическим и лабораторным работам курса.

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 образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Теория псевдослучайных генераторов»
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	основные прикладные аспекты псевдослучайных генераторов
	Умеет	разрабатывать формальные модели политик безопасности
	Владеет	навыками разработки формальных моделей политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации
(ПСК-2.1) способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает	основные определения и понятия теории псевдослучайных генераторов
	Умеет	разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации
	Владеет	основными терминами предметной области
(ПСК-2.2) способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знает	основные способы построения псевдослучайных генераторов
	Умеет	оценивать эффективность средств и методов защиты информации в компьютерных системах
	Владеет	способностью анализировать применяемые математические методы и алгоритмы
(ПСК-2.4) способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знает	принципы построения и свойства псевдослучайных генераторов
	Умеет	разрабатывать математические модели процессов
	Владеет	основными знаниями в области теории псевдослучайных генераторов

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. Основы теории псевдослучайных генераторов	ПСК-2.1, ПСК-2.2,	знает	ПР-7	1-50
			умеет	ПР-6	1-50
			владеет	ПР-6	1-50

		ПСК-2.4			
2	Раздел II. Псевдослучайные генераторы в шифровании и криптографии	ПСК-2.2, ПСК-2.4	знает	ПР-7	51-69
			умеет	ПР-6	51-69
			владеет	ПР-6	51-69

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине – зачёт и экзамен.

Для допуска к экзамену обучающийся должен получить оценку «зачтено» по всем практическим и лабораторным работам курса. Критерии оценивания практических работ представлены далее в данном Приложении. На основании сдачи работ выставляется зачёт.

Экзамен проводятся в форме собеседования (УО-1), вопросы к экзамену соответствуют темам, изучаемым на лекционных занятиях, и представлены далее в Приложении. 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 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.
- умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

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.
39. Оценочные тесты. Основные определения статистики.
40. Оценочные тесты. Подборка тестов Кнута.

41. Оценочные тесты. Подборка тестов "Diehard"
42. Оценочные тесты. Требования NIST к проверке последовательностей.
43. Оценочные тесты. Подборка тестов NIST.
44. Оценочные тесты. Частотный (монобитный) тест. Частотный тест в подпоследовательностях. Тест "дырок". Тест "блоков" в подпоследовательностях.
45. Оценочные тесты. Проверка рангов матриц. Спектральный тест. Проверка непересекающихся шаблонов. Проверка пересекающихся шаблонов.
46. Оценочные тесты. Универсальный тест Маурера. Проверка сжатия при помощи алгоритма Лемпела-Зива. Проверка линейной сложности. Проверка серий.
47. Оценочные тесты. Проверка аппроксимированной энтропии. Проверка кумулятивных сумм. Проверка случайных отклонений (базовый, расширенный тест).
48. Оценочные тесты. Другие оценочные тесты.
49. Оценка результатов тестирования.
50. Анализ статистической безопасности криптоалгоритмов.
51. Поточный шифр
52. Синхронные поточные шифры
53. Самосинхронизирующиеся поточные шифры
54. Гаммирование
55. Метод "Одноразовых блокнотов"
56. Комбинирование LSFR
57. Криптографические свойства поточных шифров
58. RC4
59. Элементная база криптосхем
60. Фильтрующие генераторы
61. Комбинирующие генераторы
62. Генераторы "δ-τ шагов"
63. Генераторы с перемежающимся шагом
64. Каскадные генераторы Голлмана
65. Сжимающие генераторы
66. Аддитивные генераторы
67. Генераторы (δ,τ)-самоусечения. Самосжимающие генераторы.
68. Генераторы Макларена-Марсальи
69. Регистры сдвига с обратной связью с переносом

На экзамене каждый экзаменационный билет содержит два вопроса из списка выше. Результаты экзамена оцениваются по четырёх балльной 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 лабораторные работы (ПР-6) и конспект (ПР-7).

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

Оценка	**Критерий**
Зачтено	Отчёт по лабораторной работе содержит все необходимые пункты (цель работы, краткий теоретический материал, задание на лабораторную работу, ход работы, полученные результаты, выводы). Оформление отчёта соответствует правилам оформления письменных работ.
Незачтено	Отчёт по лабораторной работе не содержит какого-либо необходимого пункта(ов) и/или оформление отчёта не соответствует правилам оформления письменных работ.