МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ
Декан факультета
Миронов С. В.

«31» августа 2021 г.

Рабочая программа дисциплины
Теория псевдослучайных генераторов

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Слеповичев И. И.		31.08.2021 г.
Председатель НМК	Кондратова Ю. Н.		31.08.2021 г.
Заведующий кафедрой	Абросимов М. Б.		31.08.2021 г.
Специалист Учебного управления			31.08.2021 г.

1. Цели освоения дисциплины

Целями освоения дисциплины «Теория псевдослучайных генераторов» являются формирование навыков и умений создания студентами быстрых вычислительных алгоритмов с использованием генераторов псевдослучайных чисел.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к обязательной части Блока 1 «Дисциплины (Модули)» учебного плана ООП, является дисциплиной специализации и направлена на формирование у обучающихся общепрофессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Теория вероятностей и математическая статистика», «Алгебра», «Теория информации».

Компетенции, сформированные при изучении данной дисциплины, могут быть полезны при изучении дисциплин «Модели безопасности компьютерных систем», «Теоретико-числовые методы в криптографии».

3. Результаты обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора (индикаторов) достижения компетенции**	**Результаты обучения**
ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.	ОПК-2.1.1 знает основные алгоритмы, реализующие современные математические методы защиты информации; ОПК-2.1.2 умеет применять алгоритмы, реализующие современные математические методы защиты информации; ОПК-2.1.3 владеет навыками разработки алгоритмов, реализующие современные математические методы защиты информации.	Знать термины и определения предметной области, структуру и назначение основных элементов генераторов псевдослучайных чисел, основные алгоритмы генерации последовательностей псевдослучайных чисел, методы и программные средства для проверки статистических свойств последовательностей чисел. Уметь определять статистические свойства последовательностей чисел, применять методы и алгоритмы проверки последовательностей чисел на случайность, создавать программные реализации алгоритмов генерации псевдослучайных чисел. Владеть основными языками программирования, программными средствами

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
		для создания генераторов псевдослучайных чисел.
ОПК-2.3. Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов.	ОПК-2.3.1 знает основы проведения сравнительного анализа программных и программно-аппаратных средств защиты информации; ОПК-2.3.2 умеет проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации; ОПК-2.3.3 владеет навыками проведения сравнительного анализа и осуществления обоснованного выбора программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов.	Знать структуру и назначение основных элементов генератора псевдослучайных чисел. Уметь проводить сравнительный анализ алгоритмов и программных реализаций средств генерации последовательностей псевдослучайных чисел на предмет их криптографической стойкости, а также их статистических свойств. Владеть программными средствами для создания и применения тестов проверки статистических свойств последовательностей псевдослучайных чисел.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7		8	9
1	Структура генератора псевдослучайных чисел	8	1-2	4	4	–	–	8	

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7		8	9
2	Алгоритмы генерации псевдослучайных чисел		3-6	8	8	–	–	8	Отчет по лабораторной работе №1 на 5-й неделе
3	Криптографически стойкие генераторы псевдослучайных чисел		7-10	8	8	–	–	8	Отчет по лабораторной работе №2 на 9-й неделе. Контрольная работа на 8-й неделе.
4	Тестирование статистических свойств случайных чисел		11-14	8	8	–	–	8	Отчет по лабораторной работе №3 на 13-й неделе
5	Преобразование случайных чисел к нужному распределению		15-16	4	4	–	4	8	Отчет по лабораторной работе №4 на 15-й неделе.
	Промежуточная аттестация - 36								**Экзамен**
	ИТОГО			**32**	**32**	**–**	**4**	**40**	

Содержание дисциплины

Структура генератора псевдослучайных чисел. Основные понятия. Виды генераторов случайных чисел. Стандарты и нормативные документы. Структура генератора псевдослучайных чисел. Аппаратные генераторы случайных чисел.

Алгоритмы генерации псевдослучайных чисел. Метод срединных квадратов. Линейный конгруэнтный метод. Аддитивный ГПСЧ. Метод М-последовательности (РСЛОС). Генератор Геффа. Пороговый ГПСЧ. Каскад Голлмана. Алгоритм A5. Алгоритм Fish. Алгоритм Pike. Алгоритм Mush.

ГПСЧ на базе клеточного автомата. Вихрь Мерсенна. Рэндомизация перемешиванием.

Криптографически стойкие генераторы псевдослучайных чисел. Требования к КСГПСЧ. Безопасный блочный шифр. ANSI X9.17. FIPS 186. Алгоритм генерации секретного ключа для ЭЦП. Криптографически стойкая хэш-функция. ГПСЧ использующие алгоритмы потокового шифра. ГПСЧ на основе вычислительно сложных математических задач.

Тестирование статистических свойств случайных чисел. Виды тестов. Критерий Хи-квадрат. Критерий Колмогорова-Смирнова. Эмпирические критерии: критерий равномерности (критерий частот), критерий серий, критерий интервалов, покер-критерий (критерий разбиений), критерий собирания купонов, критерий перестановок, критерий монотонности, критерий «максимум-t», критерий промежутков между днями рождений, критерий сериальной корреляции, критерий подпоследовательностей.

Преобразование случайных чисел к нужному распределению. Получение ПСЧ других распределений: распределение целых чисел, общие методы непрерывных распределений, нормальное распределение, показательное распределение, гамма-распределение порядка a>0, бета-распределение, Хи-квадрат-распределение, F-распределение, T-распределение. Целочисленные распределения: геометрическое распределение, биномиальное распределение (t,p), Пуассоновское распределение со средним мю. Случайные выборки и перемешивания.

План лабораторных занятий

На лабораторных занятиях студенты создают и тестируют генераторы псевдослучайных чисел.

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
1–2	Структура генератора псевдослучайных чисел	№1
3–6	Алгоритмы генерации псевдослучайных чисел	
7–10	Криптографически стойкие генераторы псевдослучайных чисел	№2
11–14	Тестирование статистических свойств случайных чисел	№3
15–16	Преобразование случайных чисел к нужному распределению	№4

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких образовательных технологий как создание прикладных программ и вычислительных моделей генераторов псевдослучайных чисел на языках программирования высокого уровня их демонстрация и обсуждение с

обучающимися; промежуточное тестирование, перекрестный опрос, мультимедийные презентации.

Иная контактная работа представляет собой индивидуальные консультации, оказываемые очно и дистанционно с использованием информационных и телекоммуникационных технологий с учётом образовательных возможностей обучающихся.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве. При этом основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты углубленно изучают материал раздела по соответствующей тематике недели с использованием научной и учебно-методической литературы, а также решают задания для закрепления пройденного материала.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольной работы, контрольные вопросы, вопросы для проведения промежуточной аттестации (экзамен). Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе дисциплины «Теория псевдослучайных генераторов».

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
8	10	25	0	20	0	15	30	**100**

Программа оценивания учебной деятельности студента

8 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 10 баллов.

Лабораторные занятия

Контроль выполнения лабораторных заданий в течение одного семестра – от 0 до 25 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Наличие корректно составленного отчета по самостоятельной работе оценивается от 0 до 20 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контрольная работа – от 0 до 15 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой *экзамен*, проводимый в виде устного опроса.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 21 до 30 баллов;

ответ на «хорошо» оценивается от 11 до 20 баллов;

ответ на «удовлетворительно» оценивается от 6 до 10 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 5 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за восьмой семестр по дисциплине «Теория псевдослучайных генераторов» составляет **100** баллов.

Таблица 2.1 Таблица пересчета полученной студентом суммы баллов по дисциплине «Теория псевдослучайных генераторов» в оценку (экзамен):

86–100 баллов	«отлично»
76–85 баллов	«хорошо»
60–75 баллов	«удовлетворительно»
0–59 баллов	«неудовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1) Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учеб. пособие / М. М. Глухов [и др.]. - Москва : Лань, 2011. - 394 с. : табл. - (Учебники для вузов. Специальная литература). - ISBN 978-5-8114-1116-0 : Б. ц. URL: https://e.lanbook.com/book/1540. Загл. с экрана. Яз. рус.

2) Панасенко, С. П. Алгоритмы шифрования [Текст] : спец. справ. / С. П. Панасенко. - Санкт-Петербург : БХВ-Петербург, 2009. - 564 с. : ил. - Библиогр.: с. 531-558 (408 назв.). - Предм. указ.: с. 559-564. - ISBN 978-5-9775-0319-8 (в пер.).

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: Matworks MATLAB (577478), Visual Studio 2010: Visual Studio 2010 Premium, Visual Studio 2010 Ultimate, Visual Studio Test Professional 2010, Visual Studio Team Foundation Server 2010, Visual Studio Team Explorer Everywhere 2010, Visual Studio 2010 Professional.

2) Генератор случайных чисел ГСЧ-1 [Электронный ресурс]. URL: http://tegir.ru/ml/k66.html. Загл. с экрана. Яз. рус.

3) ГОСТ Р ИСО 28640-2012. Статистические методы. Генерация случайных чисел [Электронный ресурс]. URL: http://files.stroyinf.ru/cgi-bin/ecat/ecat.fcgi?b=0&i=53898&pr=1. Загл. с экрана. Яз. рус.

4) National Institute of Standards and Technology [Электронный ресурс]. URL: https://www.nist.gov/. Загл. с экрана. Яз. рус.

5) Noisecom [Электронный ресурс]. URL: http://www.noisecom.com/. Загл. с экрана. Яз. рус.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима мультимедийная лекционная аудитория.

Для проведения лабораторных занятий необходим компьютерный класс с установленным необходимым программным обеспечением.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность специализация «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Доцент кафедры теоретических основ компьютерной безопасности и криптографии И. И. Слеповичев

Программа одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «31» августа 2021 года, протокол № 1.