Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Тестирование генераторов случайных чисел

Образовательная программа: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Курс: 3, семестр : 6

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**6**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	45
4	Лекции, час.	18
5	Практические занятия, час.	18
6	Лабораторные занятия, час.	0
7	из них в активной и интерактивной форме, час.	0
8	Аттестация, час.	2
9	Консультации, час.	7
10	Самостоятельная работа, час.	63
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	З

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.03.01 Информационная безопасность

ФГОС введен в действие приказом №1515 от 01.12.2016 г. , дата утверждения: 20.12.2016 г.

Место дисциплины в структуре учебного плана: Факультативные дисциплины, вариативная

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.03.01 Информационная безопасность

Рабочая программа обсуждена на заседании кафедры

ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

старший преподаватель, Бабичев М. М.

Заведующий кафедрой:

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

заведующий кафедрой Трушин В. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ПК.11 способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов; *в части следующих результатов обучения*:**
у1. уметь спланировать, провести эксперимент и обработать его результаты методами математической статистики

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Тестирование генераторов случайных чисел	
ПК.11.у1 уметь спланировать, провести эксперимент и обработать его результаты методами математической статистики	
1.уметь использовать вычислительные алгоритмы для оценки свойств последовательностей псевдослучайных чисел	Лекции; Практические занятия; Самостоятельная работа
2.иметь представление о возможных негативных последствиях при использовании "грязных" генераторов псевдослучайных чисел	Лекции; Самостоятельная работа
3.уметь выбирать оптимальные алгоритмы для программных генераторов случайных чисел, правильно задавать параметры генераторов и корректно их инициализировать	Лекции; Практические занятия; Самостоятельная работа
4.знать наиболее распространенные алгоритмы "чистых" генераторов псевдослучайных чисел	Лекции; Самостоятельная работа
5.уметь интерпретировать результаты статистических тестов, выраженные в форме уровней значимости (P-values)	Лекции; Практические занятия; Самостоятельная работа
6.уметь использовать пакеты статистических тестов NIST STS и Diehard для испытаний генераторов псевдослучайных чисел	Лекции; Практические занятия; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	**Активные формы, час.**	**Часы**	**Ссылки на результаты обучения**
Семестр: 6			
Дидактическая единица: Генераторы случайных чисел			
1. Основные способы генерирования шума и случайных чисел	0	2	2
2. Зачем нужно тестировать генераторы случайных чисел	0	2	2
3. Простейшие алгоритмы программных генераторов случайных чисел. Инициализация генераторов и выбор их параметров	0	2	1, 3
4. Период генератора. "Чистые" и "грязные" генераторы случайных чисел	0	2	3, 4
Дидактическая единица: Тестирование последовательностей случайных чисел			
5. Различные подходы к тестированию псевдослучайных последовательностей	0	2	1
6. Критерий согласия Пирсона хи-квадрат для проверки распределения случайных чисел на выходе генератора	0	2	1
Дидактическая единица: Пакет тестов NIST STS			
7. Пакет NIST и тесты, входящие в него	0	2	6

Дидактическая единица: Пакет тестов Diehard			
8. Пакет Diehard и тесты, входящие в него	0	2	6
Дидактическая единица: Интерпретация результатов тестирования			
9. Вероятностные критерии оценки качества псевдослучайных последовательностей	0	2	5

Таблица 3.2

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 6				
Дидактическая единица: Генераторы случайных чисел				
1. Изучение простых алгоритмов генераторов случайных чисел	0	3	3	
Дидактическая единица: Тестирование последовательностей случайных чисел				
2. Простейшие критерии оценки последовательностей псевдослучайных чисел	0	3	1	
Дидактическая единица: Пакет тестов NIST STS				
3. Использование пакета NIST для генерирования псевдослучайных чисел	0	3	6	
5. Использование пакета NIST для тестирования псевдослучайных чисел	0	3	5, 6	
Дидактическая единица: Пакет тестов Diehard				
4. Использование пакета Diehard для генерирования псевдослучайных чисел	0	3	6	
6. Использование пакета Diehard для тестирования псевдослучайных чисел	0	3	5, 6	

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 6				
1	РГЗ	3, 4	17	3
: Сборник задач по теории вероятностей, математической статистике и теории случайных функций : учебное пособие / [Б. Г. Володин и др.] ; под общ. ред. А. А. Свешникова. - СПб. [и др.], 2007. - 445 с. : ил.. - Авт. указаны на обороте тит. л..				
2	Подготовка к занятиям	2, 5	15	1
: Бабичев М. М. Пакет тестов Diehard для испытания генераторов случайных чисел [Электронный ресурс] : учебно-методическое пособие / М. М. Бабичев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2015]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000222521. - Загл. с экрана.				
3	Дополнительная учебная деятельность	6	6	0
: Сборник задач по теории вероятностей, математической статистике и теории случайных функций : учебное пособие / [Б. Г. Володин и др.] ; под общ. ред. А. А. Свешникова. - СПб. [и др.], 2007. - 445 с. : ил.. - Авт. указаны на обороте тит. л..				
4	Подготовка к аттестации	1, 2, 3, 4, 5	25	3

: Сборник задач по теории вероятностей, математической статистике и теории случайных функций : учебное пособие / [Б. Г. Володин и др.] ; под общ. ред. А. А. Свешникова. - СПб. [и др.], 2007. - 445 с. : ил.. - Авт. указаны на обороте тит. л..

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Личный типовой сайт; Социальные сети
Консультирование	e-mail; Социальные сети; Среда электронного обучения НГТУ
Контроль	e-mail; Среда электронного обучения НГТУ
Размещение учебных материалов	Личный типовой сайт; ЭБС

Таблица 5.2

Активные и интерактивные формы проведения занятий

№	Наименование активных форм
1	Дискуссия
Краткое описание применения: Можно ли создать такой пакет тестов, который давал бы 100%-ную гарантию того, что прошедший тесты генератор выдает настоящие случайные числа	

2	Дискуссия
Краткое описание применения: Зачем нужно тестировать генераторы случайных чисел	

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Мин. балл	Максимальный балл
Семестр: 6		
Практические занятия:	5	20
РГЗ:	15	40
Зачет:	15	40

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля	
		Защита РГЗ	Зачет
ПК.11	у1. уметь спланировать, провести эксперимент и обработать его результаты методами математической статистики	+	+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Кнут Д. Э. Искусство программирования. Т. 2 : пер. с англ. / Дональд Э. Кнут ; под общ. ред. Ю. В. Козаченко. - М. [и др.], 2007. - 828 с. : ил.

Дополнительная литература

1. Макконелл Д. Основы современных алгоритмов : учебное пособие по направлению "Информатика и вычислительная техника" / Дж. Макконелл ; пер. с англ. под ред. С. К. Ландо ; доп. М. В. Ульянова. - М., 2006. - 366 с. : ил.

2. Кнут Д. Э. Искусство программирования на ЭВМ. Т. 2. Получисленные алгоритмы : пер. с англ. / Д. Кнут ; под ред. К. И. Бабенко. - М., 1969. - 724 с. : ил.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Бабичев М. М. Пакет тестов Diehard для испытания генераторов случайных чисел [Электронный ресурс] : учебно-методическое пособие / М. М. Бабичев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2015]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000222521. - Загл. с экрана.

2. Сборник задач по теории вероятностей, математической статистике и теории случайных функций : учебное пособие / [Б. Г. Володин и др.] ; под общ. ред. А. А. Свешникова. - СПб. [и др.], 2007. - 445 с. : ил.. - Авт. указаны на обороте тит. л..

8.2 Специализированное программное обеспечение

1 Windows

2 Office

9. Материально-техническое обеспечение

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Компьютеры объединены в локальную сеть с выходом в Internet

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Тестирование генераторов случайных чисел

Образовательная программа: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Новосибирск - 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по **дисциплине** Тестирование генераторов случайных чисел приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ПК.11/ЭИ способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	у1. уметь спланировать, провести эксперимент и обработать его результаты методами математической статистики	Вероятностные критерии оценки качества псевдослучайных последовательностей Зачем нужно тестировать генераторы случайных чисел Использование пакета Diehard для тестирования псевдослучайных чисел Использование пакета NIST для тестирования псевдослучайных чисел Критерий согласия Пирсона хи-квадрат для проверки распределения случайных чисел на выходе генератора Основные способы генерирования шума и случайных чисел Пакет Diehard и тесты, входящие в него Пакет NIST и тесты, входящие в него Период генератора. "Чистые" и "грязные" генераторы случайных чисел Простейшие алгоритмы программных генераторов случайных чисел. Инициализация генераторов и выбор их параметров Простейшие критерии оценки последовательностей псевдослучайных чисел Различные подходы к тестированию псевдослучайных последовательностей	РГЗ	Зачет, вопросы 1, 2, 3, 4, 5, 6, 7, 8, 9

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 6 семестре - в форме зачета, который направлен на оценку сформированности компетенций ПК.11/ЭИ.

Зачет проводится в устной форме, по билетам.

Кроме того, сформированность компетенции проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 6 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе учебной дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенции ПК.11/ЭИ, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт зачета

по дисциплине «Тестирование генераторов случайных чисел», 6 семестр

1. Методика оценки

Зачет проводится в устной (письменной) форме, по билетам (тестам). Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-6, второй вопрос из диапазона вопросов 7-13 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «Тестирование генераторов случайных чисел»

---

1. Вопрос 1
2. Вопрос 2

Утверждаю: зав. кафедрой ЗИ _____ должность, ФИО
(подпись)
(дата)

2. **Критерии оценки**

- Ответ на билет (тест) для зачета считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, допускает принципиальные ошибки, оценка составляет менее 15 *баллов.*
- Ответ на билет (тест) для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, допускает непринципиальные ошибки, например, вычислительные, оценка составляет 15-25 *баллов.*
- Ответ на билет (тест) для зачета билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает значительных ошибок, оценка составляет 26-33 *баллов.*
- Ответ на билет (тест) для зачета билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен

представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок, оценка составляет 34-40 *баллов.*

3. Шкала оценки

В общей оценке по дисциплине баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** зачету **по дисциплине «**Тестирование генераторов случайных чисел**»**

1. Основные способы генерирования шума и случайных чисел
2. Зачем нужно тестировать генераторы случайных чисел
3. Простейшие алгоритмы программных генераторов псевдослучайных чисел (ПСЧ). Инициализация генераторов и выбор их параметров
4. Период генератора. "Чистые" и "грязные" генераторы случайных чисел
5. Различные подходы к тестированию псевдослучайных последовательностей
6. Критерий согласия Пирсона «хи-квадрат» для проверки распределения случайных чисел на выходе генератора
7. Пакет NIST STS и тесты, входящие в него
8. Пакет Diehard и тесты, входящие в него
9. Вероятностные критерии оценки качества псевдослучайных последовательностей (p-value)
10. История развития генераторов ПСЧ. Первые – и неудачные – алгоритмы генерирования ПСЧ
11. Алгоритм срединных квадратов для генерирования ПСЧ
12. Линейный конгруэнтный метод для генерирования ПСЧ
13. Алгоритм Парка-Миллера для генерирования ПСЧ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт
расчетно-графического задания (работы)

по дисциплине «Тестирование генераторов случайных чисел», 6 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны реализовать программный генератор псевдослучайных чисел с заданным алгоритмом на языке высокого уровня, и протестировать его с помощью одного из пакетов тестов.

Обязательные структурные части РГЗ: титульный лист, введение, теоретическая часть, листинг программы, результаты тестирования, заключение, список литературы.
Оцениваемые позиции: правильность реализации алгоритма генератора, корректность тестирования его работы.

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), программный код полностью неработоспособен, тестирование не производилось, оценка составляет менее 15 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: программный код содержит синтаксические и семантические неточности, тестирование произведено не полностью или с ошибками, оценка составляет 15-25 баллов.
- Работа считается выполненной **на базовом** уровне, если РГЗ(Р) выполнен в полном объеме, программный код не содержит существенных неточностей, тестирование проведено без существенных замечаний, оценка составляет 26-33 баллов.
- Работа считается выполненной **на продвинутом** уровне, если программный код реализован правильно и в хорошем стиле, тестирование проведено без замечаний, оценка составляет 34-40 баллов.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ(Р) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Примерный перечень тем РГЗ(Р)

1. Генератор ПСЧ (числа с плавающей запятой) с равномерным распределением в диапазоне [0;1] по методу срединных квадратов

2. Генератор ПСЧ (двоичная последовательность 0, 1…) с равномерным распределением по методу срединных квадратов

3. Генератор ПСЧ (целые числа) с равномерным распределением в диапазоне [0;100] по линейному конгруэнтному мультипликативному методу

4. Генератор ПСЧ (целые числа) с треугольным распределением в диапазоне [0;10] по линейному конгруэнтному смешанному методу

5. Генератор ПСЧ (числа с плавающей запятой) с нормальным распределением в диапазоне [-1;1] по линейному конгруэнтному мультипликативному методу