УТВЕРЖДЕНО
решением Ученого совета ФМИАТ
от «16» мая 2023 г., протокол №_4/23__
Председатель _____Волков М.А.
(подпись, расшифровка подписи)
«16___мая_____ 2023 г.

.

РАБОЧАЯ ПРОГРАММА

Дисциплина	Теория псевдослучайных генераторов
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	4

Специальность: 10.05.01 «Компьютерная безопасность»
код направления (специальности), полное наименование

Специализация: «Математические методы защиты информации»
полное наименование

Форма обучения:___очная_____
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «__01___» _____09____2023 _____ г.

Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.
Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Андреев Александр Сергеевич	ИБ и ТУ	зав.каф.,дфмн, профессор

СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину
(подпись) _Андреев А.С._ / *(Ф.И.О.)* «11_»__мая____2023 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Курс «Теория псевдослучайных генераторов» составляет одну из фундаментальных частей современной теоретической криптографии, без знания которых невозможна дальнейшая профессиональная подготовка в области современной защиты информации. При освоении данного курса у студентов формируются навыки грамотного применения теоретических основ криптографии в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

Цели освоения дисциплины:

- ознакомление студентов с основными понятиями теории генераторов псевдослучайных чисел;
- развитие навыка построения генераторов псевдослучайных чисел.

Задачи освоения дисциплины:

- овладение основными идеями и методами построения генераторов псевдослучайных чисел;
- формирование навыков грамотного применения основ теории генераторов псевдослучайных чисел в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к базовой части цикла Б1 (Б1.Б.44) образовательной программы и читается в 8-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра», «Дискретная математика», «Информатика», «Криптографические методы защиты информации».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: основные задачи и понятия криптографии; классификацию шифров по различным признакам; типы основных способов криптоанализа шифров; основные типы электронной подписи.

Дисциплина «Теория псевдослучайных генераторов» является предшествующей для прохождения преддипломной практики и итоговой государственной аттестации.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Теория псевдослучайных генераторов» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	Знать: принципы формирования программных средств криптографической защиты информации; криптографические алгоритмы и особенности их

	программной реализации; принципы функционирования сетевых протоколов, включающих криптографические алгоритмы. Уметь: разрабатывать рекомендации и предложения по совершенствованию и повышению эффективности защиты информации Владеть: методами отладки создаваемых средств защиты
ОПК-2.2. Способен разрабатывать и анализировать математические модели механизмов защиты информации	Знать: принципы построения средств криптографической защиты информации; криптографические протоколы, применяемые в компьютерных сетях; Уметь выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы Владеть: методами разработки математических моделей, реализуемых в средствах защиты информации удалённых атак на ОИС и основные методы защиты от них

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 6**.**

4.2. Объем дисциплины по видам учебной работы:

Вид учебной работы	Количество часов (форма обучения - дневная)	
	Всего по плану	В т.ч. по семестрам
		7
Контактная работа обучающихся с преподавателем	126	54
Аудиторные занятия:		
• Лекции	72	36

• Практические и семинарские занятия		
• Лабораторные работы (лабораторный практикум)	54	36
*Самостоятельная работа	54	18
Виды промежуточной аттестации (экзамен, зачет)		зачет
		8
Аудиторные занятия:		
Лекции		36
Практические и семинарские занятия		
Лабораторные работы (лабораторный практикум)		18
Самостоятельная работа		36
Контроль	36	36
Всего часов по дисциплине	216	216
Форма текущего контроля знаний и контроля самостоятельной работы		Лабораторные работы, проверка решения задач
Виды промежуточной аттестации (экзамен, зачет)		экзамен
Общая трудоемкость в зач. ед.	6	6

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы:

Форма обучения _____очная_____

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			

1	2	3	4	5	6	7	
Раздел 1. Конгруэнтные генераторы							
1. Введение.	2	1				1	Домашние задания
2. Линейный конгруэнтный генератор	8	3		4	2	1	Лабораторная работа. Домашние задания
3. Полиномиальный конгруэнтный генератор	3	2				1	Домашние задания
Раздел 2. Генераторы на основе регистра сдвига с линейной обратной связью							
4. Регистры сдвига с линейной обратной связью.	7	4		2		1	Домашние задания
5. Регистры сдвига с линейной обратной связью по переносу.	10	4		4	1	2	Лабораторная работа. Домашние задания
6. Генератор Фиббоначи.	13	4		6	1	3	Лабораторная работа. Домашние задания
7. Генератор Галуа	11	4		4	1	3	Лабораторная работа. Домашние задания
8. Генератор Геффе	10	4		4	1	2	Лабораторная работа. Домашние задания
9. Пороговый генератор	12	4		6	1	2	Лабораторная работа. Домашние задания
10. Генератор «Стоп-пошел»	15	6		6	1	3	Лабораторная работа. Домашние задания
11. Самопрорежива ющие генераторы	7	2		1	1	4	Лабораторная работа. Домашние задания
12. Сжимающие генераторы	7	2		1	1	4	Лабораторная работа.

							Домашние задания
Раздел 3. Криптографически стойкие генераторы							
13. Безопасный блочный шифр.	14	4		2	1	8	Лабораторная работа. Домашние задания
14. Генераторы на основе алгоритмов потокового шифра.	12	4		2	1	6	Лабораторная работа. Домашние задания
15. Генераторы на основе вычислительно сложных математических задач.	14	4				10	Домашние задания
16. Генераторы на основе односторонней функции	20	6		4	2	10	Лабораторная работа. Домашние задания
Раздел 4. Тестирование качества генераторов							
17. Графические тесты качества ПСЧП	30	8		4	2	18	Лабораторная работа. Домашние задания
18. Статистические тесты качества ПСЧП	22	6		4	2	12	Лабораторная работа. Домашние задания
ВСЕГО	216	72		54	18	90	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Конгруэнтные генераторы

Тема 1. Введение.

Генераторы случайных чисел. Два класса методов генерации случайных чисел. Требования к генератору псевдослучайных чисел. Среднеквадратичный ГПСЧ.

Тема 2. Линейный конгруэнтный генератор.

Формула линейного конгруэнтного метода. Теорема о периоде последовательности, формируемой линейным конгруэнтным генератором. Мультипликативные генераторы. Теорема о максимальном периоде последовательности, генерируемой мультипликативным генератором. Обобщение линейного конгруэнтного генератора. Потенциал линейной конгруэнтной последовательности с максимальным периодом. Инверсный конгруэнтный генератор. Теорема о максимальном периоде инверсного конгруэнтного генератора. Недостатки линейных конгруэтных генераторов.

Тема 3. Полиномиальный конгруэнтный генератор.

Квадратичный, кубический и полиномиальный конгруэнтные генераторы.

Раздел 2. Генераторы на основе регистра сдвига с линейной обратной связью

Тема 4. Регистры сдвига с линейной обратной связью.

Регистр сдвига. Регистр сдвига с линейной обратной связью. Отводная последовательность битов. Примитивные многочлены. Условие максимальности периода последовательности на основе РСЛОС. Частные случаи РСЛОС.

Тема 5. Регистры сдвига с линейной обратной связью по переносу.

Схема работы РСЛОСП. Максимальный период последовательности генератора РСЛОСП

Тема 6. Генератор Фибоначчи.

Аддитивные генераторы ПСЧ. Генератор Фибоначчи. Разновидность генератора, предложенная G. Mitchell и D. Moore в 1958 году. Теорема о максимальном периоде последовательности, формируемой аддитивным ГСПЧ Фибоначчи с запаздыванием. Обобщение аддитивного ГСПЧ. Теорема о периоде обобщенного аддитивного ГСПЧ. Выбор коэффициентов.

Тема 7. Генератор Галуа.

Тема 8. Генератор Геффе.

Схема генератора Геффа. Длина периода генератора Геффа. Линейная сложность генератора Геффа.

Тема 9. Пороговый генератор.

Схема порогового генератора. Линейная сложность порогового генератора. Недостатки порогового генератора.

Тема 10. Генератор «Стоп-пошел».

Схема генератора «Стоп-пошел». Алгоритм генерации последовательности. Период последовательности генератора «Стоп-пошел». Чередующийся генератор «Стоп-пошел». Двухсторонний генератор «Стоп-пошел». Каскад Голлмана. Схема каскада Голлмана. Линейная сложность последовательности генератора. Свойства каскада Голлмана.

Тема 11. Самопрореживающие генераторы.

Прореживаемые генераторы. Модификация. Схема самопрореживающего генератора. Свойства самопрореживающего генератора.

Тема 12. Сжимающие генераторы.

Схема сжимающего генератора. Линейная сложность последовательности сжимающего генератора. Период последовательности сжимающего генератора.

Раздел 3. Криптографически стойкие генераторы

Тема 13. Безопасный блочный шифр.

Особенности блочного шифрования. Недостатки блочного шифрования. Режимы блочного шифрования, применяемые для построения ГПСП. ГПСП на основе ГОСТ 28147-89 в режиме Counter. Преобразования и раундовая функция ГПСП ГОСТ 28147-89. ГПСП на основе AES-128. Преобразования и раундовая функция AES-128. Основные особенности AES-128.

Тема 14. Генераторы на основе алгоритмов потокового шифра.

Особенности поточного шифрования. Режимы поточного шифрования для построения ГПСП. Приемы построения ГПСП при использовании поточных шифров. ГПСП на основе RC4 в режиме OFB.

Тема 15. Генераторы на основе вычислительно сложных математических задач.

Сложно-теоретический подход к построению генератора. Генератор Шамира, генератор Blum-Micali.

Тема 16. Генераторы на основе односторонней функции.

Понятие односторонней функции. Кандидаты в односторонние функции. Односторонние функции с секретом. Требования к односторонней функции. ГПСП BBS. Достоинства и

недостатки ГПСП BBS. ГПСП RSA.

Раздел 4. Тестирование качества генераторов
Тема 17. Графические тесты качества ПСЧП.
Гистограмма распределения элементов ПСЧП. Распределение элементов на плоскости. Проверка серий, монотонности. Построение профиля линейной сложности.
Тема 18. Статистические тесты качества ПСЧП.
Тест несцепленных серий. Проверка интервалов, комбинаций, перестановок, монотонности, корреляции.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены учебным планом дисциплины.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Подробное задание к лабораторным работам дано в учебно-методическом пособии: Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с. - **URL:** ftp://10.2.96.134/Text/Amiranov_2016.pdf

Раздел 1. Конгруэнтные генераторы
Тема 2. Линейный конгруэнтный генератор.
Цель работы: ознакомиться с методом построения конгруэнтного генератора.
Задание. Написать программу, реализующую алгоритм генерации последовательности псевдослучайных чисел используя конгруэнтный генератор.
Варианты задания.

1. Разработать программу генерации псевдослучайных чисел по формуле линейного конгруэнтного генератора смешанного типа.
2. Разработать программу генерации псевдослучайных чисел по формуле линейного мультипликативного конгруэнтного генератора.
3. Разработать программу генерации псевдослучайных чисел по формуле инверсного конгруэнтного генератора.

Методические указания: параметры генератора подобрать из условия максимальности периода последовательности, используя соответствующую теорему.

Раздел 2. Генераторы на основе регистра сдвига с линейной обратной связью
Тема 5. Регистры сдвига с линейной обратной связью по переносу.
Тема 6. Генератор Фиббоначи.
Цель работы: ознакомиться с методом построения генератора Фиббоначи.
Задание. Написать программу, реализующую алгоритм генерации последовательности псевдослучайных чисел используя конгруэнтный генератор Фиббоначи.
Варианты задания.

1. Разработать программу генерации псевдослучайных чисел по формуле аддитивного генератора Фибоначчи с запаздыванием.
2. Разработать программу генерации псевдослучайных чисел по формуле аддитивного генератора Фибоначчи обобщенного типа.

Раздел 2. Генераторы на основе регистра сдвига с линейной обратной связью
Тема 7. Генератор Галуа
Тема 8. Генератор Геффе
Тема 9. Пороговый генератор
Тема 10. Генератор «Стоп-пошел»
Тема 11. Самопрореживающие генераторы
Тема 12. Сжимающие генераторы

Цель работы: ознакомиться с методом построения заданного генератора.
Задание. Написать программу, реализующую алгоритм генерации последовательности псевдослучайных чисел используя заданный генератор.
Варианты задания.

1. Разработать программу генерации псевдослучайных чисел по формуле: Генератор Геффа.
2. Разработать программу генерации псевдослучайных чисел по формуле: Генератор «Стоп-пошел».
3. Разработать программу генерации псевдослучайных чисел по формуле: Чередующийся генератор «Стоп-пошел».
4. Разработать программу генерации псевдослучайных чисел по формуле: Двухсторонний генератор «Стоп-пошел».
5. Разработать программу генерации псевдослучайных чисел по формуле: Каскад Голлмана из трех РСЛОС.
6. Разработать программу генерации псевдослучайных чисел по формуле: Сжимающий генератор.
7. Разработать программу генерации псевдослучайных чисел по формуле: Пороговый генератор из трех РСЛОС.

Методические указания: основное внимание должно быть уделено освоению методам построения генераторов РСЛОС.

Раздел 3. Криптографически стойкие генераторы
Тема 13. Безопасный блочный шифр.
Цель работы: Освоение методов построения криптостойких ГПСП на основе блочного шифрования.
Задание: реализация криптографических ГПСП с использованием функций блочных шифров.
Методические указания: основное внимание должно быть уделено освоению методам построения криптостойких ГПСП на основе блочного шифрования.
Тема 14. Генераторы на основе алгоритмов потокового шифра.
Цель работы: Освоение методов построения криптостойких ГПСП на основе поточного шифрования.
Задание: реализация криптографических ГПСП с использованием функций поточных шифров.
Методические указания: основное внимание должно быть уделено освоению методам построения криптостойких ГПСП на основе поточного шифрования.
Тема 16. Генераторы на основе односторонней функции.
Цель работы: Освоение методов построения криптостойких ГПСП на основе

односторонних функций.
Задание: реализация криптографических ГПСП с использованием односторонних функций.
Методические указания: основное внимание должно быть уделено освоению методам построения криптостойких ГПСП на основе односторонних функций.

Раздел 4. Тестирование качества генераторов
Тема 17. Графические тесты качества ПСЧП.
Цель работы: ознакомиться с графическими тестами качества ПСЧП.
Задание. Написать программу, реализующую графическую проверку качества ПСЧП.
Методические указания: основное внимание должно быть уделено освоению методов проведения графических тестов качества ПСЧП.
Тема 18. Статистические тесты качества ПСЧП.
Цель работы: ознакомиться со статистическими тестами качества ПСЧП.
Задание. Написать программу, реализующую статическую проверку качества ПСЧП.
Методические указания: основное внимание должно быть уделено освоению методов проведения статистических тестов качества ПСЧП.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Курсовые, контрольные работы и рефераты не предусмотрены учебным планом дисциплины.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Генераторы случайных чисел. Два класса методов генерации случайных чисел. Требования к генератору псевдослучайных чисел. Среднеквадратичный ГПСЧ.
2. Формула линейного конгруэнтного метода. Теорема о периоде последовательности, формируемой линейным конгруэнтным генератором.
3. Мультипликативные генераторы. Теорема о максимальном периоде последовательности, генерируемой мультипликативным генератором.
4. Обобщение линейного конгруэнтного генератора. Потенциал линейной конгруэнтной последовательности с максимальным периодом.
5. Инверсный конгруэнтный генератор. Теорема о максимальном периоде инверсного конгруэнтного генератора. Недостатки линейных конгруэнтных генераторов.
6. Квадратичный, кубический и полиномиальный конгруэнтные генераторы.
7. Регистр сдвига. Регистр сдвига с линейной обратной связью. Отводная последовательность битов. Примитивные многочлены. Условие максимальности периода последовательности на основе РСЛОС.
8. Частные случаи РСЛОС.
9. Схема работы РСЛОСП. Максимальный период последовательности генератора РСЛОСП
10. Аддитивные генераторы ПСЧ. Генератор Фибоначчи. Разновидность генератора, предложенная G. Mitchell и D. Moore в 1958 году. Теорема о максимальном периоде последовательности, формируемой аддитивным ГСПЧ Фибоначчи с запаздыванием.
11. Обобщение аддитивного ГСПЧ. Теорема о периоде обобщенного аддитивного ГСПЧ. Выбор коэффициентов.
12. Генератор Галуа.

13. Генератор Геффе.
14. Пороговый генератор.
15. Генератор «Стоп-пошел».

10. ПЕРЕЧЕНЬ ВОПРОСОВ к экзамену

1. Генераторы случайных чисел. Два класса методов генерации случайных чисел. Требования к генератору псевдослучайных чисел. Среднеквадратичный ГПСЧ.
2. Формула линейного конгруэнтного метода. Теорема о периоде последовательности, формируемой линейным конгруэнтным генератором.
3. Мультипликативные генераторы. Теорема о максимальном периоде последовательности, генерируемой мультипликативным генератором.
4. Обобщение линейного конгруэнтного генератора. Потенциал линейной конгруэнтной последовательности с максимальным периодом.
5. Инверсный конгруэнтный генератор. Теорема о максимальном периоде инверсного конгруэнтного генератора. Недостатки линейных конгруэнтных генераторов.
6. Квадратичный, кубический и полиномиальный конгруэнтные генераторы.
7. Регистр сдвига. Регистр сдвига с линейной обратной связью. Отводная последовательность битов. Примитивные многочлены. Условие максимальности периода последовательности на основе РСЛОС.
8. Частные случаи РСЛОС.
9. Схема работы РСЛОСП. Максимальный период последовательности генератора РСЛОСП
10. Аддитивные генераторы ПСЧ. Генератор Фибоначчи. Разновидность генератора, предложенная G. Mitchell и D. Moore в 1958 году. Теорема о максимальном периоде последовательности, формируемой аддитивным ГСПЧ Фибоначчи с запаздыванием.
11. Обобщение аддитивного ГСПЧ. Теорема о периоде обобщенного аддитивного ГСПЧ. Выбор коэффициентов.
12. Генератор Галуа.
13. Генератор Геффе.
14. Пороговый генератор.
15. Генератор «Стоп-пошел».
16. Чередующийся генератор «Стоп-пошел». Двухсторонний генератор «Стоп-пошел».
17. Каскад Голлмана.
18. Самопрореживающие генераторы.
19. Сжимающие генераторы.
20. Безопасный блочный шифр.
21. Генераторы на основе алгоритмов потокового шифра.
22. Генераторы на основе вычислительно сложных математических задач..
23. Генераторы на основе односторонней функции.
24. Графические тесты качества ПСЧП.
25. Статистические тесты качества ПСЧП.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Конгруэнтные генераторы 1. Введение.	Проработка учебного материала, подготовка к сдаче зачета	1	Зачет
Конгруэнтные генераторы 2. Линейный конгруэнтный генератор	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	4	Зачет, проверка лабораторных работ, проверка решения домашних задач
Конгруэнтные генераторы 3. Полиномиальный конгруэнтный генератор	Проработка учебного материала, подготовка к сдаче зачета, решение домашних задач	3	Зачет, проверка решения домашних задач
Генераторы на основе регистра сдвига с линейной обратной связью 4. Регистры сдвига с линейной обратной связью.	Проработка учебного материала, подготовка к сдаче зачета, решение домашних задач	4	Зачет, проверка решения домашних задач
Генераторы на основе регистра сдвига с линейной обратной связью 5. Регистры сдвига с линейной обратной связью по переносу.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	2	Зачет, проверка лабораторных работ, проверка решения домашних задач
Генераторы на основе регистра сдвига с линейной обратной связью 6. Генератор Фибоначчи.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	2	Зачет, проверка лабораторных работ, проверка решения домашних задач
Генераторы на основе регистра сдвига с линейной обратной связью 7. Генератор Галуа	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	1	Зачет, проверка лабораторных работ, проверка решения домашних задач
Генераторы на основе регистра сдвига с линейной обратной связью 8. Генератор Геффе	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	2	Зачет, проверка лабораторных работ, проверка решения домашних задач
Генераторы на основе регистра сдвига с линейной обратной	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета,	2	Зачет, проверка лабораторных работ, проверка решения

связью 9. Пороговый генератор	решение домашних задач		домашних задач
Генераторы на основе регистра сдвига с линейной обратной связью 10. Генератор «Стоп-пошел»	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	3	Зачет, проверка лабораторных работ, проверка решения домашних задач
Генераторы на основе регистра сдвига с линейной обратной связью 11. Самопрореживающие генераторы	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	2	Зачет, проверка лабораторных работ, проверка решения домашних задач
Генераторы на основе регистра сдвига с линейной обратной связью 12. Сжимающие генераторы	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	6	Зачет, проверка лабораторных работ, проверка решения домашних задач
Криптографически стойкие генераторы 13. Безопасный блочный шифр.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	6	Зачет, проверка лабораторных работ, проверка решения домашних задач
Криптографически стойкие генераторы 14. Генераторы на основе алгоритмов потокового шифра.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	8	Зачет, проверка лабораторных работ, проверка решения домашних задач
Криптографически стойкие генераторы 15.Генераторы на основе вычислительно сложных математических задач.	Проработка учебного материала, подготовка к сдаче зачета, решение домашних задач	10	Зачет, проверка решения домашних задач
Криптографически стойкие генераторы 16. Генераторы на основе односторонней функции	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	12	Зачет, проверка лабораторных работ, проверка решения домашних задач
Тестирование качества генераторов 17.Графические тесты качества ПСЧП	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета, решение домашних задач	12	Зачет, проверка лабораторных работ, проверка решения домашних задач
Тестирование качества генераторов 18. Статистические	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета,	12	Зачет, проверка лабораторных работ, проверка решения

тесты качества ПСЧП	решение домашних задач		домашних задач

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Кнут Д.Э. Искусство программирования, том 2. Получисленные алгоритмы, 3-е изд. – М.: Издательский дом «Вильямс», 2017. – 832 с.
2. Стохастические методы и средства защиты информации в компьютерных системах и сетях / М. А. Иванов [и др.]; под ред. И. Ю. Жукова. - Москва: Кудиц-Пресс, 2009. - 512 с. : ил. - Библиогр.: с. 504-510. - ISBN 978-5-91136-068-9 (в пер.) : 75.00..
3. Краснов М.В. Математические методы защиты информации. Ч. 3: методические указания / сост. М. В. Краснов; Яросл. Гос. Ун-т им. П. Г. Демидова. – Ярославль: ЯрГУ, 2013. – 48 с.

Дополнительная

1. Поднебесова Г.Б. Абстрактная и компьютерная алгебра [Электронный ресурс]: практикум/ Поднебесова Г.Б.— Электрон. текстовые данные.— Челябинск: Южно-Уральский государственный гуманитарно-педагогический университет, 2016.— 125 с. — Режим доступа: http://www.iprbookshop.ru/83852.html
2. ГОСТ-Эксперт – единая база ГОСТов Российской Федерации для образования и промышленности:
   2.1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012.
   2.2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013.

3.Аппаратный генератор случайных чисел ГСЧ-6. [Электронный ресурс]. – Режим доступа: http://tegur.ru/ml//k66.html. Проверено 29.07.2016.

4 ГОСТ Р ИСО 28640-2012. [Электронный ресурс]. – Режим доступа: http:// files.stroyinf.ru/cgi-bin/ecat/ecat.fcgi?b=0&i=53898&pr=1. Проверено 29.07.2016. http://www.noisecom.com. [Электронный ресурс]. – Режим доступа: Проверено 29.07.2016.

5. Шнайер Б. 16.1 Алгоритм ГОСТ 28147-89 // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols. Algorithms and Source Code in C. – М.: Триумф, 2002. – С. 373-377.

учебно-методическая

1. Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с. - **URL:** ftp://10.2.96.134/Text/Amiranov_2016.pdf

3. Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий, Каф. информ. безопасности и теории управления. - Ульяновск : УлГУ, 2017. -Загл. с экрана. - Электрон. текстовые дан. (1 файл : 352 КБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/915

4. Андреев А. С. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", "Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", "Системный анализ и управление" / А. С. Андреев, С. М. Бородин, А. М. Иванцов; УлГУ, ФМиИТ. - Ульяновск :УлГУ, 2015. - Загл. с экрана; Имеется печ. аналог. - Электрон. текстовые дан. (1 файл : 14, 7 Мб). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/297

5. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Теория псевдослучайных генераторов» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2019. - 7 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/10711.

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. /___ _____/___04.05.2023_____/
должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Инженер ведущий	/ Щуренко Ю.В.	/	/ 04.05.2023
Должность сотрудника УИТТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитория должна быть укомплектована специализированной мебелью, учебной доской, мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающимся) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических возможностей:

- для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

/ _____ / Андреев А.С. /
(подпись) (Ф.И.О.)

«_11_» ___05_____2023_ г.