Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП:

_____ Н.А. Семыкина

«__9__» ___06___ 2023 г.

Рабочая программа дисциплины (с аннотацией)

Теория псевдослучайных генераторов

Специальность

10.05.01 Компьютерная безопасность

Специализация

Математические методы защиты информации

Для студентов 4 курса очной формы обучения

Уровень высшего образования

СПЕЦИАЛИТЕТ

Составитель:

к. ф.-м. н. доц. Сушкин В.В.

Тверь 2023

I. Аннотация.

1. Наименование дисциплины в соответствии с учебным планом

«Теория псевдослучайных генераторов».

2. Цель и задачи дисциплины.

Целью освоения дисциплины является:

подготовка к работе в сфере защиты информации..

Задачами освоения дисциплины являются:

знакомство с основами теории псевдослучайных генераторов;
приобретение навыков проектирования информационных моделей, предполагающих использование генераторов псевдослучайных чисел.

3. Место дисциплины в структуре ООП.

Дисциплина относится
к дисциплинам вариативной части.

Необходимым для изучения дисциплины является материал, который рассматривается в рамках следующих дисциплин: ”Математическая логика и теория алгоритмов”, ”Алгебра”, ”Теория вероятностей и математическая статистика”, ”Языки программирования”.Освоение дисциплины необходимо как предшествующее для следующих дисциплин: ”Принципы оптимальности в моделях защиты информации” и ”Теоретико-игровые методы в защите информации” .

4. Объем дисциплины:

4 зачетных единицы, **144** академических часа, **в том числе**

контактная работа: лекции **36** часов, практические занятия **36** часов,
самостоятельная работа: 72 часа.

5. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

Планируемые результаты освоения образовательной программы (формируемые компетенции).	**Планируемые результаты обучения по дисциплине.**
ПК-14 - способность организовывать работы по	**Владеть:** методами формирования требований по защите информации. **Уметь:** применять отечественные и зарубежные стандарты в области компьютерной безопасности для

выполнению режима защиты информации, в том числе ограниченного доступа.	проектирования, разработки и оценивания защищенности компьютерной системы. **Знать:** способы поиска и обработки информации по профилю деятельности.
ПК-15 - способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы.	**Владеть:** методами управления информационной безопасностью информационных систем. **Уметь:** пользоваться современной научно-технической информацией по исследуемым проблемам и задачам. **Знать:** способы поиска и обработки информации по профилю деятельности.
ПСК-2.2. способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	**Владеть:** математическим аппаратом, информационными и компьютерными технологиями из данного курса. **Уметь:** проводить предварительное оценивание временной сложности разрабатываемых алгоритмов, применять изученные математические и компьютерные методы при решении профессиональных задач. **Знать:** принципы построения псевдослучайных генераторов и их свойства, соответствующие разделы курса.

6. Форма промежуточной аттестации: экзамен.
7. Язык преподавания русский**.**

II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.

1. Для студентов очной формы обучения.

Учебная программа – наименование разделов и тем.	Всего (час).	Контактная работа (час).	Самостоятельная

			Лекции.	Практические занятия.	работа (час).
1	Линейный конгруэнтный генератор.	16	6	6	4
2	Квадратичный и кубический конгруэнтные генераторы.	15	6	6	3
3	Обобщённый линейный конгруэнтный генератор.	16	6	6	4
4	Регистры сдвига с линейной обратной связью. Конфигурация Галуа.	15	6	6	3
5	Генератор Геффе, использующий три регистра сдвига с линейной обратной связью.	7	3	3	1
6	Обобщённый генератор Геффе.	7	3	3	1
7	Пороговый генератор.	7	3	3	1
8	Генераторы «стоп-пошёл». Каскад Голлманна.	7	3	3	1
ИТОГО		90	36	36	18

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.

В качестве заданий для самостоятельной работы студентов предполагается, в частности, использовать задания из [2] и [3] (см. раздел V, список ”Дополнительная литература”).

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.

Типовые контрольные задания для проверки уровня сформированности компетенций.

Этап формирования компетенции, в котором участвует дисциплина.	Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера).	Показатели и критерии оценивания компетенции, шкала оценивания.
Базовый, **владеть.**	1) Используя значения параметров линейного конгруэнтного генератора, выяснить, является ли длина периода последовательности псевдослучайных чисел, формируемой генератором, максимальной. 2) Используя значения параметров обобщённого линейного конгруэнтного генератора, найти максимально возможное значение длины периода последовательности псевдослучайных чисел, формируемой генератором.	Задание полностью выполнено – 7 баллов. Наличие отдельных ошибок – 3 - 6 баллов. Большое количество ошибок – 0 баллов.
Базовый, **уметь.**	1) Найти период последовательности псевдослучайных чисел, формируемой заданным линейным конгруэнтным генератором. 2) Найти период последовательности псевдослучайных чисел, формируемой заданным обобщённым линейным конгруэнтным генератором.	Задание полностью выполнено – 6 баллов. Наличие отдельных ошибок – 3 - 5 баллов. Большое количество ошибок – 0 баллов.
Базовый, **знать.**	1) Привести определение понятия генератора последовательности псевдослучайных чисел. 2) Привести определение понятия периода последовательности псевдослучайных чисел.	Глубокие знания – 4 балла. Неуверенные знания – 2 - 3 балла. Серьезные пробелы в знаниях – 0 баллов.

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) Основная литература

1. Непейвода Н. Н. Стили и методы программирования : учебное пособие / Н. Н. Непейвода. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. - 295 с. – Режим доступа: http://www.iprbookshop.ru/102065.html

2. Методы программирования: учебное пособие / Ю.Ю. Громов, О.Г. Иванова, Ю.В. Кулаков и др.; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2012. - 144 с.: табл., схем. - Библиогр. в кн. - ISBN 978-5-8265-1076-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=437089

б) Дополнительная литература:

1. Гниденко И. Г. Технологии и методы программирования : учебное пособие для вузов / И. Г. Гниденко, Ф. Ф. Павлов, Д. Ю. Федоров. - Электрон. дан. - Москва : Юрайт, 2021. - 235 с. - (Высшее образование). - Режим доступа: https://urait.ru/bcode/469759

2. Клименко И. С. Информационная безопасность и защита информации: модели и методы управления : Монография / И. С. Клименко; Северо-Кавказский федеральный университет, ф-л в г. Пятигорске. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2024. - 180 с. - (Научная мысль). - Дополнительное профессиональное образование. – Режим доступа: https://znanium.com/catalog/document?id=4313467

Сырецкий Г.А. Моделирование систем. Часть 2. Интеллектуальные системы [Электронный ресурс]: учебное пособие/ Г.А. Сырецкий.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2010.— 80 с.— Режим доступа: http://www.iprbookshop.ru/45401.html

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.
2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.
3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.
4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.
5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.

VII. Методические указания для обучающихся по освоению дисциплины.

Требования к рейтинг-контролю.

Модули.	Темы.	Виды контроля.	Максимальное количество баллов.	Формы контрольных испытаний.
Модуль I.	№ 1 (из учебной программы).	Текущий.	15	1) контроль посещения занятий, 2) устный опрос.
		Рубежный.	15	1) устный опрос, 2) контрольная работа.
Модуль II.	№ 3 (из учебной программы).	Текущий.	15	1) контроль посещения занятий, 2) устный опрос.
		Рубежный.	15	1) устный опрос, 2) контрольная работа.
		Итоговый контроль (экзамен).	40	1) ответ по билету, 2) контрольное задание.

VIII. Перечень педагогических и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (по необходимости):

1) проведение лекционных занятий в аудитории и в компьютерном классе,
2) выполнение студентами индивидуальных заданий на практических занятиях в компьютерном классе,
3) использование необходимого программного обеспечения

Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus	бесплатно
OpenOffice	бесплатно
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

.

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски. Класс ПЭВМ класса Intel с установленным программным обеспечением для организации самостоятельной работы.

X. Сведения об обновлении рабочей программы дисциплины.

№п.п.	Обновленный	Описание внесенных	Дата и протокол заседания

	раздел рабочей программы дисциплины.	изменений.	кафедры, утвердившего изменения.