Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 2023 г.

Рабочая программа дисциплины (с аннотацией)

Теория псевдослучайных генераторов

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 4 курса ОФО

Составитель:
Сушкин В. В.

Тверь 2023

I. Аннотация

1. 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.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Алгебра», «Математический анализ».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 3 зачетные единицы, 108 академических часов, в том числе:

контактная аудиторная работа: лекции – 30 часов, в т.ч. практическая подготовка – 0 часов; практические занятия – 30 часов, в т.ч. практическая подготовка – 5 часов;

самостоятельная работа: 48 часов.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.	**ОПК-2.1.1.** Использует в профессиональной деятельности криптографические алгоритмы и реализует их программно.
	ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации.
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.	**ОПК-3.13.** Обосновывает классические положения и стандартные методы теории вероятностей и случайных процессов, а также математической статистики.
	ОПК-3.14. Разрабатывает вероятностные и статистические модели при решении типовых прикладных задач.

5. Форма промежуточной аттестации и семестр прохождения – зачет в 8 семестре.

6. Язык преподавания русский.

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

Очная форма обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)			Самостоятельная работа, в том числе контроль (час.)
		Лекции	Практические занятия		
			всего	в т.ч. практическая подготовка	
Тема 1. Последовательности псевдослучайных чисел и генераторы последовательностей псевдослучайных чисел. Основные понятия.	22	6	6	1	10
Тема 2. Утверждения о необходимых и достаточных условиях принадлежности упорядоченного числового набора множеству периодов последовательности псевдослучайных чисел.	43	12	12	2	19
Тема 3. Утверждения о длине периода последовательностей псевдослучайных чисел: а) о допустимых значениях длины периода и б) о последовательностях с периодом максимальной длины.	43	12	12	2	19
ИТОГО	108	30	30	5	48

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии

Тема 1. Последовательности псевдослучайных чисел и генераторы последовательностей псевдослучайных чисел. Основные понятия.	Лекция, практическое занятие.	Проблемная лекция, дискуссионные технологии, технология развития креативного мышления, дистанционные образовательные технологии.
Тема 2. Утверждения о необходимых и достаточных условиях принадлежности упорядоченного числового набора множеству периодов последовательности псевдослучайных чисел.	Лекция, практическое занятие.	Проблемная лекция, дискуссионные технологии, технология развития креативного мышления, дистанционные образовательные технологии.
Тема 3. Утверждения о длине периода последовательностей псевдослучайных чисел: а) о допустимых значениях длины периода и б) о последовательностях с периодом максимальной длины.	Лекция, практическое занятие.	Проблемная лекция, дискуссионные технологии, технология развития креативного мышления, методы группового решения творческих задач, дистанционные образовательные технологии.

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения <u>текущей аттестации</u>

<u>Задания для практических (семинарских) занятий</u>

Тема I.

Задание 1 (ОПК-2.1.1, ОПК-2.1.2).

Допустим, X – последовательность псевдослучайных чисел, Y – последовательность $\{Y_i\}_{i\in\{0,1,\ldots,9\}}$ действительных чисел, определяемая следующим образом

$Y_0 = 17$, $Y_1 = 31$, $Y_2 = 19$, $Y_3 = 5$, $Y_4 = 23$,

$Y_5 = 2$, $Y_6 = 37$, $Y_7 = 3$, $Y_8 = 7$, $Y_9 = 11$,

и пусть 11 – это стартовая позиция последовательности Y.

Определить, чему равно значение X_{1000}.

Задание 2 (ОПК-2.1.1, ОПК-2.1.2).

Допустим, X – последовательность псевдослучайных чисел, Y – последовательность $\{Y_i\}_{i\in\{0,1,\ldots,9\}}$ действительных чисел, определяемая следующим образом

$Y_0 = 17$, $Y_1 = 31$, $Y_2 = 19$, $Y_3 = 5$, $Y_4 = 23$,

$Y_5 = 2$, $Y_6 = 37$, $Y_7 = 3$, $Y_8 = 7$, $Y_9 = 11$,

и пусть 17 – это стартовая позиция последовательности Y.

Определить, чему равно значение X_{1000}.

Тема II.

Задание 1 (ОПК-2.1.1, ОПК-2.1.2).

Допустим, X – это последовательность псевдослучайных чисел, определяемая следующим образом

$X_0 = 1,\ \ X_1 = 0,\ \ X_2 = 0,\ \ X_3 = 1,$

$X_n = F(X_{n-4}, X_{n-3}, X_{n-2}, X_{n-1}), n \in \{ 4, 5, \dots \},$

где F – это некоторая функция с областью определения $\{0, 1\}\times\{0, 1\}\times\{0, 1\}\times\{0, 1\}$ и множеством значений в $\{0, 1\}$.

Известно, что

$X_4 = 1,\ \ X_5 = 0,\ \ X_6 = 1,\ \ X_7 = 0,\ \ X_8 = 1,\ \ X_9 = 1,\ \ X_{10} = 1,\ \ X_{11} = 0,\ \ X_{12} = 1,$

$X_{13} = 0,\ \ X_{14} = 1.$

Необходимо найти, по крайней мере, один период последовательности X.

Задание 2 (ОПК-2.1.1, ОПК-2.1.2).

Допустим, X – это последовательность псевдослучайных чисел, определяемая следующим образом

$X_0 = 0,\ \ X_1 = 1,\ \ X_2 = 0,\ \ X_3 = 0,$

$X_n = F(X_{n-4}, X_{n-3}, X_{n-2}, X_{n-1}), n \in \{ 4, 5, \dots \},$

где F – это некоторая функция с областью определения $\{0, 1\}\times\{0, 1\}\times\{0, 1\}\times\{0, 1\}$ и множеством значений в $\{0, 1\}$.

Известно, что

$X_4 = 1,\ \ X_5 = 1,\ \ X_6 = 0,\ \ X_7 = 1,\ \ X_8 = 0,\ \ X_9 = 1,\ \ X_{10} = 1,\ \ X_{11} = 1,\ \ X_{12} = 0,$

$X_{13} = 1,\ \ X_{14} = 0,\ \ X_{15} = 1.$

Необходимо найти наименьшую из стартовых позиций периодов последовательности X.

Тема III.

Задание 1 (ОПК-3.13, ОПК-3.14).

Допустим, X – это последовательность псевдослучайных чисел, удовлетворяющая условиям

$X_n \in \{0, 1\}, n \in \{ 0, 1, 2, 3 \},$

$X_n = F(X_{n-4}, X_{n-3}, X_{n-2}, X_{n-1}), n \in \{ 4, 5, \dots \},$

где F – это некоторая функция с областью определения $\{0, 1\}\times\{0, 1\}\times\{0, 1\}\times\{0, 1\}$ и множеством значений в $\{0, 1\}$.

Доказать, что длина периода последовательности X не может быть равна 17.

Задание 2 (ОПК-3.13, ОПК-3.14).

Допустим, X – это последовательность псевдослучайных чисел, удовлетворяющая условиям

$X_n \in \{0, 1, 2\}, n \in \{ 0, 1, 2 \},$

$X_n = (X_{n-3} + X_{n-2}) \bmod 3, n \in \{ 3, 4, \dots \}.$

Доказать, что длина периода последовательности X не может быть равна 27.

Оценочные материалы для проведения <u>промежуточной аттестации</u>

Проверяемые индикаторы достижения компетенций: ОПК-2.1.1, ОПК-2.1.2, ОПК-3.13, ОПК-3.14.

Каждый студент решает индивидуальное задание и отвечает на теоретический вопрос.

Примерные вопросы к зачету

1. Понятие последовательности псевдослучайных чисел и понятие генератора последовательностей псевдослучайных чисел.

2. Понятие квазипериода последовательности псевдослучайных чисел (и его длины). Понятие стартовой позиции квазипериода.
3. Понятие периода последовательности псевдослучайных чисел (и его длины). Понятие стартовой позиции периода.
4. Множество периодов последовательности псевдослучайных чисел и способы его отыскания.
5. Множество допустимых значений для длины периода последовательности псевдослучайных чисел. Основные утверждения.
6. Линейный конгруэнтный генератор. Утверждение об условиях формирования последовательности (имеется в виду значения генератора) с периодом максимальной длины.
7. Квадратичный конгруэнтный генератор. Утверждение об условиях формирования последовательности (имеется в виду значения генератора) с периодом максимальной длины.

Вид и способ проведения промежуточной аттестации: индивидуальный устный опрос сочетается с самостоятельной практической работой студента.

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – **3** балла. Для получения зачета необходимо выполнить задачу и ответить на теоретический вопрос с суммарной оценкой не менее 2-х балов.

3 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется полное верное решение задачи, включающее правильный ответ.

2 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Дано верное решение задачи, но в решении имеются неверные записи И/ИЛИ арифметические ошибки.

1 балл:

Ответ демонстрирует знание и корректное использование терминологии. Решение содержит фактические ошибки, не искажающие общего смысла.

0 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ ответ содержит существенные фактические ошибки, искажающие смысл. Решение не дано ИЛИ дано неверное решение.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

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

2) Программное обеспечение

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

3) Современные профессиональные базы данных и информационные справочные системы

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.

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации по организации самостоятельной работы студентов

На лекциях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам.

Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить, что часы для самостоятельной работы из всего объема времени, затраченного на дисциплину, будут превосходить иные виды работ. Важно продумать стиль фиксации нового и важного материала.

Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте и в личном кабинете электронной образовательной среды (LMS).

Требования к рейтинг-контролю для студентов очной формы обучения.

Текущая работа студентов очной формы обучения оценивается в 100 баллов, которые распределяются между двумя модулями (периодами обучения) следующим образом:

Модуль (период обучения)	Максимальная сумма баллов в модуле	Максимальная сумма баллов за работу на практических занятиях	Реферирование, представление научной статьи, создание и отладка кода	Максимальный балл за рейтинговую контрольную работу
1	50	18	12	20
2	50	18	12	20

Правила формирования рейтинговой оценки и шкалу пересчета рейтинговых баллов в оценку на экзамене см. в «Положении о рейтинговой системе обучения в ТвГУ»: https://tversu.ru/sveden/files/204-R_Pologhenie_o_reytingovoy_sisteme_obucheniya_v_TvGU.pdf

VII. Материально-техническое обеспечение

Учебный процесс по данной дисциплине проводится в аудиториях, оснащенных мультимедийными средствами обучения. Для организации самостоятельной работы студентов необходимо наличие персональных компьютеров с доступом в Интернет.

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**

Помещение для самостоятельной работы, учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, практики *компьютерный класс* 203а, 170002, г.Тверь, Садовый пер-к, д. 35.	Столы, стулья, переносной ноутбук, компьютеры.	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
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации у*чебная аудитория* 203, 224, 170002, г.Тверь, Садовый пер-к, д. 35.	Столы, стулья, переносной ноутбук, проектор.	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

Наличие учебно-наглядных пособий, презентаций для проведения занятий лекционного и семинарского типа, обеспечивающих тематические иллюстрации.

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	Обновленный раздел рабочей программы дисциплины	Описание внесенных изменений	Реквизиты документа, утвердившего изменения
1	I - VIII	Корректировка всех разделов в соответствии с новым стандартом.	Протокол № 10 от 29.06.2021.
2	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023
3	II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий, IV. Оценочные материалы для проведения текущей и промежуточной аттестации	Корректировка наименований разделов и тем. Корректировка оценочных материалов	Протокол № 7 от 7.03.2024