

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Смирнов Сергей Николаевич  
Должность: врио ректора  
Дата подписания: 16.10.2024 11:24:28  
Уникальный программный ключ:  
69e375c64f7e975d4e8890e

**Министерство науки и высшего образования РФ**  
**Федеральное государственное бюджетное образовательное**  
**учреждение высшего образования**  
**«Тверской государственный университет»**

Рассмотрено и рекомендовано  
на заседании Ученого совета  
математического факультета  
протокол № 9 от 28.05.2024г.

«УТВЕРЖДАЮ»:  
Руководитель ООП  
Н.А. Семькина



«28» мая 2024 г.



**ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА**

Специальность  
10.05.01 Компьютерная безопасность

Специализация  
Математические методы защиты информации

Уровень высшего образования  
СПЕЦИАЛИТЕТ

Тверь 2024 г

## **Пояснительная записка**

Экзамен является междисциплинарным, проводится в соответствии с графиком учебного процесса. Цель экзамена – проверка овладения выпускником основных компетенций, требуемых в профессиональной деятельности.

К участию в государственном экзамене допускаются студенты, полностью выполнившие учебный план и не имеющие академической задолженности.

Экзамен может проводиться за один или несколько дней в зависимости от количества студентов, допущенных для его прохождения.

Экзамен проводится в устной форме. Каждый билет содержит два теоретических вопроса и одну задачу по теме, входящей в программу итогового квалификационного экзамена. В качестве вопросов формулируются основные теоретические положения, предполагающие их развернутое обоснование при ответе.

Время, выделяемое на подготовку ответов и выполнение задания – 1 час. Ответ студента производится в форме выступления перед членами Государственной экзаменационной комиссии, допускается использование записей, сделанных студентом при подготовке к ответу на вопросы комиссии. Продолжительность ответа 10-15 минут. Членами государственной экзаменационной комиссии студенту могут быть заданы дополнительные вопросы, относящиеся к дисциплинам, входящим в программу государственного экзамена.

## **Перечень компетенций, уровень сформированности которых будет оцениваться на экзамене**

**ОПК-2.** способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов.

**ПК-5.** способностью участвовать в разработке и конфигурировании

программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

**ПК-7.** способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем.

**ПК-15.** способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы.

**ПСК-2.1.** способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации.

**ПСК-2.2.** способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах.

**ПСК-2.3.** способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.

**ПСК-2.5.** способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

### **Требования к профессиональной подготовленности специалиста.**

Математик, специалист по компьютерной безопасности, должен знать и уметь использовать:

- основные понятия и методы математического анализа, геометрии, алгебры, теории функций комплексного переменного, теории вероятностей и математической статистики;

- математические модели простейших систем и процессов в естествознании и технике;

- вероятностные модели для конкретных процессов и явлений, проводить

необходимые расчеты в рамках построенной модели;

- основные понятия и методы математической логики и теории алгоритмов, теории передачи информации, теории кодирования;

- современные методы программирования и методы разработки эффективных алгоритмов решения прикладных задач;

- принципы и методы организационной защиты информации в различных сферах деятельности государства;

- принципы построения современных систем защиты информации в компьютерных системах;

- руководящие документы по оценке защищенности компьютерных систем;

- методы проведения анализа надежности системы защиты информации в компьютерных системах;

- принципы построения современных криптографических систем;

- методы криптографического анализа типовых криптографических алгоритмов и протоколов;

- стандарты в области криптографической защиты информации;

- основные правовые понятия по проблемам информационной безопасности и защиты информации; владеть:

- методами разработки и исследования моделей надежности и безопасности компьютерных систем;

- методами организации деятельности подразделений защиты информации;

- методикой разработки нормативно-методических документов по организационной защите информации;

- методами определения организационных и технических каналов утечки информации.

### **Критерии оценки итогового государственного экзамена**

Оценка ответа на вопрос (выполненного задания) выставляется членами Государственной экзаменационной комиссии.

Возможные оценки на государственном экзамене: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Результаты проведения

государственного экзамена оглашаются после окончания государственного экзамена в день его проведения.

Отметка **«ОТЛИЧНО»**. Ответ студента полный и правильный, содержит четкие формулировки и подтверждается примерами. Студент уверенно отвечает на дополнительные вопросы, свободно ориентируется в вопросах билета. Материал изложен в определенной логической последовательности, литературным языком, с использованием современных научных терминов; ответ самостоятельный.

Отметка **«ХОРОШО»**. Ответ студента правильный. Студент показал знание основного программного материала. Студент испытывает незначительные трудности в ответах на дополнительные вопросы. Материал изложен в определенной логической последовательности, при этом допущены 2-3 незначительные погрешности, исправленные по требованию экзаменатора. Соблюдены нормы литературной речи. Ответ самостоятельный.

Отметка **«УДОВЛЕТВОРИТЕЛЬНО»**. Студент показал поверхностные знания вопросов билета в объеме, необходимом для предстоящей работы по профессии. Ответ недостаточно логически выстроен, самостоятелен. Основные понятия употреблены правильно, но обнаруживается недостаточное раскрытие теоретического материала. Студент испытывает достаточные трудности в ответах на дополнительные вопросы. Научная терминология используется недостаточно, незначительные нарушения норм литературной речи.

**Фонды оценочных средств**  
**для государственной итоговой аттестации**

**Теоретические вопросы для проверки уровня сформированности**  
**компетенции ОПК - 2.**

***Математический анализ***

1. Определение предела числовой последовательности. Единственность предела. Ограниченность сходящейся последовательности. Арифметические операции над сходящимися последовательностями. Предел монотонной последовательности. Признак Вейерштрасса сходимости монотонной последовательности. Число  $e$ .
2. Понятие производной. Производные основных элементарных функций. Геометрический смысл производной. Правила дифференцирования. Дифференцирование сложной функции. Таблица производных.
3. Определение и свойства неопределенного интеграла. Основные методы интегрирования. Таблица интегралов.
4. Определение и свойства определенного интеграла. Интеграл с переменным верхним пределом. Формула Ньютона–Лейбница.
5. Определение и свойства числовых рядов. Необходимое условие сходимости ряда. Ряды с положительными членами. Признаки Даламбера и Коши сходимости числовых рядов.
6. Поточечная и равномерная сходимость функциональных последовательностей. Равномерная сходимость функциональных рядов. Мажорантный признак Вейерштрасса.

***Геометрия***

1. Различные виды уравнения прямой на плоскости и в пространстве. Расстояние от точки до прямой на плоскости. Угол между двумя прямыми.
2. Скалярное, векторное, смешанное произведение векторов в пространстве, их свойства, выражение через координаты сомножителей.
3. Определение кривых второго порядка, их канонические уравнения. Эксцентриситет, директрисы кривых второго порядка, теорема об эксцентриситете

***Алгебра***

1. Матрицы и операции над ними. Определители матриц и их свойства. Определитель произведения матриц. Критерий обратимости матриц. Ранг матрицы над полем, способы его вычисления. Ранг произведения матриц. Обратная матрица и способы ее вычисления.

2. Системы линейных уравнений над полем. Критерий Кронекера-Капелли. Алгоритм Гаусса. Фундаментальная система решений однородной системы линейных уравнений. Общее решение системы линейных уравнений.
3. Кольца вычетов. Малая теорема Ферма. Сравнения первой степени.
4. Кольцо многочленов над кольцом с единицей. Делимость многочленов с остатком. Теорема Безу. Делимость многочленов над полем. Наибольший общий делитель (НОД) и наименьшее общее кратное многочленов. Взаимно простые многочлены и их свойства. Неприводимые многочлены и их свойства. Каноническое разложение многочлена и его однозначность
5. Группы и их основные свойства. Смежные классы по подгруппе, теорема Лагранжа. Циклические группы. Четные и нечетные подстановки конечных множеств. Теорема Кэли. Нормальные делители группы. Факторгруппа, теорема об эпиморфизме.
6. Векторные пространства над полем, их базисы и размерность. Координаты векторов в базисе и их изменение при переходе к другому базису. Свойства конечномерных векторных пространств. Подпространства векторного пространства, операции над ними. Размерности суммы и пересечения подпространств.
7. Линейное преобразование векторного пространства, его матрица в данном базисе, примеры. Критерии обратимости преобразования. Характеристический многочлен линейного преобразования. Собственные значения и собственные векторы преобразования, инвариантные подпространства.
8. Евклидово пространство. Существование ортонормированного базиса. Ортогональное дополнение подпространства.
9. Квадратичная форма над полем, ее матрица и ранг, канонический вид над полем действительных чисел. Положительно определенные квадратичные формы.
10. Конечные поля, характеристика поля, число элементов, теорема о примитивном элементе. Существование поля с заданным примарным числом элементов. Описание подполей. Неприводимые многочлены над конечными полями. Существование неприводимых многочленов данной степени над конечным полем.

### *Дискретная математика*

1. Булевы функции, их суперпозиция. Полные системы булевых функций. Примеры полных систем. Замкнутые классы булевых функций. Общий критерий полноты.
2. Автоматные языки, примеры. Необходимые условия автоматности языка. Автоматность однословного и конечного языка. Пример неавтоматного языка.

### ***Математическая логика и теория алгоритмов***

1. Булевы функции. Представление булевых функций формулами алгебры высказываний. Замкнутые классы функций. Критерии полноты для булевых функций.
2. Исчисления высказываний и предикатов, их полнота и непротиворечивость.
3. Основные подходы к формализации понятия алгоритма: машины Тьюринга, рекурсивные функции.
4. Понятие сложности алгоритма. Классы сложности.

### ***Теория вероятностей и математическая статистика***

1. Вероятностное пространство. Аксиомы вероятности. Свойства вероятности меры. Дискретное вероятностное пространство. Классическое определение вероятностей
2. Случайные величины. Функции распределения и их свойства. Абсолютно непрерывные, дискретные распределения. Типовые распределения: биномиальное, равномерное, геометрическое, пуассоновское, нормальное, показательное.
3. Условные вероятности. Независимость событий. Формула полной вероятности. Формула Байеса.
4. Математическое ожидание случайной величины и его свойства. Вычисление математических ожиданий для типовых распределений. Дисперсия случайной величины и ее свойства. Коэффициент корреляции и его свойства.
5. Теорема Пуассона. Локальная предельная теорема Муавра-Лапласа. Примеры.
6. Основные понятия математической статистики: понятия генеральной совокупности, выборки, дискретного вариационного ряда, эмпирической функции распределения, выборочных моментов. Примеры использования этих понятий в практических задачах.
7. Основные методы статистического оценивания. Метод моментов. Метод максимального правдоподобия. Применение к случаю нормального и биномиального распределения.

### ***Теория информации и кодирования***

1. Энтропия и ее свойства. Количество информации. Общая схема линии связи.
2. Взаимная информация. Информационная дивергенция.
3. Оптимальное кодирование. Корректирующие свойства кодов. Линейный код и способы его задания.



**Практические вопросы для проверки уровня сформированности  
компетенции ОПК - 2.**

1. Даны вершины треугольника  $A(12;-4)$ ,  $B(0;5)$ ,  $C(-12;-11)$ . Составьте уравнение его высоты и медианы, проведенных из вершины  $B$ .
2. Составьте каноническое уравнение прямой, проходящей через точку  $M(1;2;-3)$  параллельно прямой

$$\begin{cases} 3x - y + 2z - 7 = 0, \\ x - 3y - 4z + 3 = 0. \end{cases}$$

3. Составьте уравнение касательной к параболе  $y^2=8x$ , параллельной прямой  $2x+2y-3=0$ .
4. Найдите проекцию точки  $Q(5, 4)$  на прямую, проходящую через точки  $A(-2;3)$  и  $B(6; -3)$ .

5. Исследовать на сходимость числовой ряд  $\sum_{n=1}^{\infty} \frac{2^n n!}{n^n}$ .

6. Исследовать на сходимость числовой ряд  $\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n(n+1)^2}$ .

7. Исследовать на сходимость числовой ряд  $\sum_{n=1}^{\infty} \frac{2n-1}{3^n}$ .

8. Вычислить неопределенный интеграл  $J = \int \frac{dx}{(x-1)(x-2)}$ .

9. Вычислить определенный интеграл  $J = \int_0^{\pi} x^2 \sin x dx$ .

10. Найдите собственные значения (числа) и собственные векторы линейного

преобразования, заданного матрицей  $\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$

11. Найти матрицу  $X = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix}$ . При условии, что

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} = \begin{pmatrix} 31 & 40 \\ 7 & 10 \\ 16 & 22 \end{pmatrix}$$

12. Найти общее решение системы уравнений и какую-нибудь её фундаментальную систему решений

$$\begin{cases} x_1 + x_3 = 0 \\ x_2 + x_6 = 0 \\ x_3 + x_6 = 0 \\ x_4 + x_7 = 0 \end{cases}$$

13. Выясните, какая из следующих формул логики предикатов тождественно истина, а какая – нет. Результат обоснуйте.

a)  $\neg \forall x \exists y P(x, y) \rightarrow \forall y \exists x P(x, y)$ ;

b)  $\exists x P(x) \wedge \exists x Q(x) \rightarrow \exists x (P(x) \wedge Q(x))$ .

14. С помощью основных равносильностей приведите формулу логики высказываний

$$\neg(p \rightarrow \neg(q \rightarrow \neg r \vee p)) \wedge (q \rightarrow p \wedge r)$$

к дизъюнктивной нормальной форме. Результат проверьте построением истинностных таблиц для исходной и полученной формул.

15. Обосновав результат, запишите формулу логики высказываний  $\phi(p, q, r)$ , имеющую следующую таблицу истинности:

$p$	И	И	И	И	Л	Л	Л	Л
$q$	И	И	Л	Л	И	И	Л	Л
$r$	И	Л	И	Л	И	Л	И	Л
$\phi(p, q, r)$	И	Л	Л	И	Л	И	Л	Л

Результат обоснуйте.

16. Решить экстремальную задачу.

$$x_1^2 + x_2^2 \rightarrow \min,$$

$$2x_1 + x_2 \geq 2, \quad 2x_1 + x_2 \leq 8,$$

$$x_1 + x_2 \geq 6, \quad x_1 \geq 0, \quad x_2 \geq 0.$$

17. Решить экстремальную задачу.

$$x_1 + 2x_2 \rightarrow \max,$$

$$3x_1^2 + x_2^2 \leq 1,$$

$$x_1 - 8x_2 \leq -1, \quad x_1 \geq 0, \quad x_2 \geq 0.$$

18. Решить экстремальную задачу.

$$1 - x_1 \rightarrow \min,$$

$$(1 - x_1)^3 - x_2 \geq 0,$$

$$x_1 \geq 0, \quad x_2 \geq 0.$$

**Теоретические вопросы для проверки уровня сформированности компетенций ПК - 5, ПК - 7, ПК - 15, ПСК - 2.1, ПСК - 2.2, ПСК - 2.3, ПСК-2.5.**

***Системы управления базами данных***

1. Проектирование баз данных. E-R диаграммы. Нормальные формы отношений. Нормализация.
2. Реляционная алгебра. Основные определения, операторы. Реализационная полнота языка SQL.

***Теория кодирования, сжатия и восстановления информации***

1. Циклический код. Теорема существования. Порождающая и проверочная матрицы. Систематические кодеры.
2. Декодирование циклического кода. Синдромное декодирование. Общий алгоритм обнаружения и исправления ошибок.
3. Сжатие информации. Универсальные методы сжатия информации. Классы методов сжатия. Технические характеристики процесса сжатия данных.

***Методы алгебраической геометрии в криптографии***

1. Понятие эллиптической кривой над числовым полем. Законы сложения точек кривой и построение группы точек кривой.
2. Эллиптические кривые в криптографии. Электронная цифровая подпись на эллиптических кривых.

***Модели управляемых систем. Оптимизация искусственных нейронных сетей***

1. Применение искусственных нейронных сетей в информационной и компьютерной безопасности. Динамические нейронные сети и методы их исследования.
2. Нейронные сети и проблемы искусственного интеллекта. Классификация ИНС. Способы обучения ИНС.

***Управление нелинейными системами***

1. Задачи нелинейного программирования. Метод множителей Лагранжа.
2. Постановка задачи оптимального управления динамической системой. Линейные управляемые модели.
3. Принцип максимума Л.С. Понтрягина. Краевая задача.
4. Численные методы и алгоритмы построения оптимального решения управления нелинейными системами.

***Теория псевдослучайных генераторов***

1. Необходимые и достаточные условия принадлежности упорядоченного числового набора множеству периодов последовательности псевдослучайных чисел.

2. Утверждения о множестве допустимых значений для длины периода последовательности псевдослучайных чисел.

### ***Криптографические методы защиты информации***

1. Криптосистемы с открытым ключом. Понятие сертификата. Криптосистема RSA. Выбор параметров.

2. Блочные шрифты.

### **Практические вопросы для проверки уровня сформированности компетенций ПК- 5 , ПК- 7 , П К -15, ПСК-2.1, ПСК - 2.2, ПСК - 2.3, ПСК - 2.5.**

#### ***Системы управления базами данных***

1. Структура базы данных «Учредительство» содержит следующие таблицы:

- «Лицо» — *Код, ФИО, Дата рождения. Месторождения, Паспортные данные;*
- «Организация» — *Код ОКПО, Наименование, Условное наименование, Профиль деятельности (Производственный, Коммерческий, Посреднический, научно-производственный), Организационная форма (ЗАО, ОАО, и т. д.). Код Руководителя, Код глав. бухгалтера, Телефон;*
- «Учредительство»—*Код, Код учредителя-лица, Код учредителя-организации, Код учрежденной организации, Дата учреждения, Данные документа учредительства, Доля капитала, Форма капитала;*
- «Адрес» — *Код, Код Лица, Код Организации, Город, Район, Улица, № дома, № квартиры, Дата начала, Дата окончания.*

Вводом и корректировкой данных занимаются несколько сотрудников, за каждым из которых закрепляется регистрация и ведение БД по различным организационным формам, профилю деятельности и району размещения регистрируемых организации. Для работы и доступа только к «своим» данным составьте представления объектов (таблиц) базы данных сотруднику Петрову, отвечающему за регистрацию посреднических акционерных обществ, размещающихся в Железнодорожном районе, и предоставьте ему соответствующий доступ.

2. В базе данных «Штаты подразделений» содержатся следующие таблицы:

- «Сотрудники» — *Таб.№, ФИО, Подразделение, Должность (шт. категория);*
- «Штатные категории» — *Код категории, Наименование (Начальник отдела. Зам. начальника отдела. Начальник сектора, Ведущий инженер. Старший инженер. Инженер, Техник), должностной оклад;*
- «Подразделения» — *№№, Наименование, Руководитель;*
- «Штаты» — *№№ подразделения, Код штатной категории, Количество должностей.*

База данных необходима для обеспечения работы руководителей структурных подразделений (справочные функции), сотрудников отдела кадров (ведение базы данных) и бухгалтерии (использование в начислении заработной платы). Составьте и обоснуйте целесообразную систему рабочих групп пользователей и таблицу доступа к объектам базы данных.

3. В базе данных «Преподаватели и занятия» содержатся следующие таблицы:

- «Преподаватели» — *Таб.№, ФИО, Кафедра (Истории, Архивоведения, Документоведения), Должность (Зав.каф, Профессор, Преподаватель, Ассистент), Ученая степень (Кандидат наук, Доктор наук), Ученое звание (Старший научный сотрудник, Доцент, Профессор, Академик);*
- «Контракты/Труд.Соглашения» — *№№. Код Преподавателя, Дата заключения, Срок действия, Ставка, Особые условия;*
- «Дисциплины» — *Код дисциплины, Наименование, Количество часов в учебном плане, Форма отчетности (Экзамен, Дифференцированный зачет. Зачет);*
- «Занятия» — *Дата, Время (1-я пара, 2-я пара, 3-я пара, 4-я пара). Аудитория, Вид (Лекция, Практическое занятие, Семинар, Лабораторная работа. Экзамен, Зачет), Преподаватель, Дисциплина, Код уч. группы;*
- «Итоги сессии» — *Код, Семестр, Код дисциплины, Код Студента, Отметка, Код Преподавателя*
- «Учебные группы» — *Код группы (И101, И102, И103, И104, И105 и т.д.), Специализация (История, Архивоведение, Документоведение),*

*Таб.№\_старосты, Таб.№№\_куратора; • «Студенты» — Таб.№№, ФИО, Год рождения, Уч. группа, Отметка о переводе на след.курс.*

База данных необходима для методистов учебного отдела (составление и ведение расписания занятий, учетная работа по распределению студентов по группам, итогам сессий), профессорско-преподавательскому составу (справки по расписанию занятий), работникам отдела кадров (ведение установочных данных по преподавателям и студентам), студентам (справки по расписанию занятий). Составьте и обоснуйте целесообразную систему рабочих групп пользователей и таблицу доступа к объектам базы данных.

### ***Теория кодирования, сжатия и восстановление информации***

1. Построить циклический код длины 7 с порождающим многочленом

$$g(x) = x^4 + x^2 + x + 1.$$

Найти его проверочный многочлен. Найти порождающую и проверочную матрицу.

2. Алфавит содержит 7 букв, которые встречаются с вероятностями 0,3; 0,2; 0,2; 0,1; 0,1; 0,07; 0,03. Провести кодирование, используя методику Хаффмена.

3. Выполнить сжатие сообщения методом кодирования серии последовательностей с управляющим байтом (метод RLE). С помощью таблицы CP-1251 перевести символы заданной фразы в десятичные числа, а затем десятичные числа перевести в двоичные.

Текст сообщения: **КОД 222221333.**

### ***Методы алгебраической геометрии в криптографии***

1. Даны точки  $P(13,16)$ ,  $Q(17,3)$ ,  $R(18,20)$  на кривой  $E_{23}(1,1)$ .

Найти точку  $2P + Q - R$ .

2. Дана эллиптическая кривая  $E_{11}(1,6)$ . Найти все точки эллиптической кривой, определить ее порядок и образующий элемент.

### ***Модели управляемых систем. Оптимизация искусственных нейронных сетей.***

1. Электрическая или химическая нейронная модель взаимодействия нейронов описывается системой дифференциальных уравнений:

$$\begin{aligned} \dot{x}_i(t) &= -\lambda \left[ 1 + R \exp(-x_i^2(t)) \right] x_i(t) + \\ &+ \frac{1}{n-1} \sum_{j=1}^n w_{ij}(t) (x_j(t) - x_i(t)) \text{ если } \sum_{i=1}^n x_i < M, \\ \dot{x}_i(t) &= 0, \text{ если } \sum_{i=1}^n x_i \geq M, \\ x_i(0) &= a_i, \quad i = \overline{1, n}, \\ |w_{ij}(t)| &\leq a_{ij}, \quad i, j = \overline{1, n}, \text{ п.в. } t \in [0, T], \end{aligned}$$

Весовые коэффициенты  $w_{ij}(t)$ ,  $i, j = \overline{1, n}$ , определяющие влияние  $j$ -го нейрона на  $i$ -й, выбираются из условия минимума функционала  $I(w(\cdot))$ , в котором подынтегральная функция выбирается в зависимости от программы обучения. Эта функция, характеризует общую энергию нейронной сети и корреляцию с заданным состоянием системы:

$$\begin{aligned} J(w) &= \int_0^T \left[ \sum_{i=1}^n \sum_{j=1}^n \alpha_{ij} w_{ij}^2(t) + \sum_{i=1}^n \varepsilon_i (x_i(t) - \psi(t))^2 \right] dt + \\ &+ \sum_{i=1}^n M_i (x_i(T) - A_i)^2 + \sum_{i=1}^n c_i x_i(T). \end{aligned}$$

Построить краевую задачу принципа максимума для данной модели нейронной сети.

### *Управление нелинейными системами*

1. Используя метод множителей Лагранжа решить экстремальную задачу.

$$2x_1 + x_2 \rightarrow \min,$$

$$x_1^2 + 4x_2^2 \leq 1.$$

2. Построить краевую задачу принципа максимума для следующей задачи оптимального управления

$$\int_{t_0}^T x(t) dt \rightarrow \max,$$

$$\dot{x}(t) = -ax + bu(t) \left[ 1 - \frac{x(t)}{M} \right],$$

$$x(t_0) = S_0,$$

$$0 \leq u(t) \leq A,$$

3. В следующей задаче выписать необходимые условия оптимальности и найти оптимальное управление, используя принципа максимума Понтрягина.



$$J(u) = \int_0^T (x_1^2(t) + u^2(t))dt + x_2(T) \rightarrow \inf,$$

$$\dot{x}_1(t) = x_1^2(t) - x_2(t) - u(t)x_1(t),$$

$$\dot{x}_2(t) = x_1(t)x_2(t),$$

$$x_i(0) = A_i, \quad i=1,2,$$

$$0 \leq u(t) \leq 1.$$

### *Теория псевдослучайных генераторов*

1. Используя значения параметров линейного конгруэнтного генератора, выяснить, является ли длина периода последовательности псевдослучайных чисел, формируемой генератором, максимальной.

- а) Модуль  $m = 11$ , Множитель  $a = 5$ ,  
 Приращение  $c = 3$ , Начальное значение  $x_0 = 1$ .
- б) Модуль  $m = 16$ , Множитель  $a = 5$ ,  
 Приращение  $c = 3$ , Начальное значение  $x_0 = 1$ .

2. Используя значения параметров линейного конгруэнтного генератора, найти максимально возможное значение длины периода последовательности псевдослучайных чисел, формируемой генератором.

- а) Модуль  $m = 5$ , Множитель  $a = 6$ ,  
 Приращение  $c = 7$ , Начальное значение  $x_0 = 2$ .
- б) Модуль  $m = 11$ , Множитель  $a = 5$ ,  
 Приращение  $c = 3$ , Начальное значение  $x_0 = 1$ .

### *Теоретико-игровые методы в защите информации*

1. Допустим, в бескоалиционной игре  $\Gamma$ , описывающей процесс закупки средств защиты для компьютерной системы,

$$n = 4, \quad m = 3,$$

$$(c_1 \ c_2 \ c_3 \ c_4) = (2,5 \ 1,2 \ 1,5 \ 2,2),$$

$$\begin{pmatrix} p_{13} & p_{23} & p_{33} & p_{43} \\ p_{12} & p_{22} & p_{32} & p_{42} \\ p_{11} & p_{21} & p_{31} & p_{41} \end{pmatrix} = \begin{pmatrix} 0,85 & 0,4 & 0,5 & 0,8 \\ 0,75 & 0,5 & 0,6 & 0,65 \\ 0,9 & 0,3 & 0,4 & 0,85 \end{pmatrix},$$

здесь

$n$  – это число средств защиты (для компьютерной системы), имеющихся в

продаже; средства защиты пронумерованы числами от 1 до  $n$ ;

$m$  – число типов атак, которые могут быть использованы при нападении на компьютерную систему; типы атак пронумерованы числами от 1 до  $m$ ;

$c_i, i \in \{1, 2, \dots, n\}$ , – стоимость  $i$ -го средства защиты;

$p_{ij}, i \in \{1, 2, \dots, n\}, j \in \{1, 2, \dots, m\}$ , – вероятность отражения атаки  $j$ -го типа  $i$ -м средством защиты.

Положим, множества  $S'$  и  $S''$ , равные соответственно  $\{1, 2\}$  и  $\{3, 4\}$ , являются стратегиями игрока, ответственного за обеспечение безопасности компьютерной системы. Необходимо, выяснить, какое из следующих условий выполнено

- 1) стратегия  $S'$  доминируется стратегией  $S''$ ,
- 2) стратегия  $S''$  доминируется стратегией  $S'$ ,
- 3) стратегии  $S'$  и  $S''$  не доминируются друг другом.

2. Допустим, в бескоалиционной игре  $\Gamma$ , описывающей процесс закупки средств защиты для компьютерной системы,

$n = 3, d = 0,3, m = 3,$

$(c_1 c_2 c_3) = (0,1; 0,11; 0,12)$

$(w_1 w_2 w_3) = (1 \quad 1 \quad 1),$

$$\begin{pmatrix} p_{13} & p_{23} & p_{33} \\ p_{12} & p_{22} & p_{32} \\ p_{11} & p_{21} & p_{31} \end{pmatrix} = \begin{pmatrix} 0,1 & 0,2 & 0,3 \\ 0,3 & 0,1 & 0,2 \\ 0,2 & 0,3 & 0,1125 \end{pmatrix},$$

здесь

$n$  – это число средств защиты (для компьютерной системы), имеющих в продаже; средства защиты пронумерованы числами от 1 до  $n$ ;

$c_i, i \in \{1, 2, \dots, n\}$ , – стоимость  $i$ -го средства защиты;

$d$  – максимальный объём денежных средств, который может быть потрачен на приобретение средств защиты;

$m$  – число типов атак, которые могут быть использованы при нападении на компьютерную систему; типы атак пронумерованы числами от 1 до  $m$ ;

$w_j, j \in \{1, 2, \dots, m\}$ , – наибольший суммарный ущерб, который может быть причинён при использовании атак  $j$ -го типа;

$p_{ij}, i \in \{1, 2, \dots, n\}, j \in \{1, 2, \dots, m\}$ , – вероятность отражения атаки  $j$ -го типа  $i$ -м средством защиты.

Необходимо найти множество недоминируемых максиминных стратегий игрока, ответственного за обеспечение безопасности компьютерной системы.

1. Найти ключ шифра аффинного преобразования

$$y \equiv Lx \pmod{32}.$$

Цифровое представление открытого текста в кольце  $Z_{32}$ :  $x_1=(7,8,12)$ ,  $x_2=(13,5,5)$ ,  
 $x_3=(17,14,11)$ ,  $x_4=(13,22,5)$ .

Цифровое представление закрытого текста в кольце  $Z_{32}$ :  $y_1=(5,30,24)$ ,  $y_2=(19,17,3)$ ,  
 $y_3=(19,12,17)$ ,  $y_4=(23,12,23)$ .

2. Найти ключ шифра аффинного преобразования

$$y=Lx+a \pmod{32}.$$

Цифровое представление открытого текста в кольце  $Z_{32}$ :  $x_1=(5,30,24)$ ,  $x_2=(19,17,3)$ ,  
 $x_3=(19,12,17)$ ,  $x_4=(23,12,23)$ .

Цифровое представление закрытого текста в кольце  $Z_{32}$ :  $y_1=(7,8,12)$ ,  $y_2=(13,5,5)$ ,  
 $y_3=(17,14,11)$ ,  $y_4=(13,22,5)$ .

3. С помощью S-блока:

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

преобразовать двоичный вектор 011001 в 4-рех битное целое.

## ЛИТЕРАТУРА, РЕКОМЕНДУЕМАЯ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Фихтенгольц Г. М. Курс дифференциального и интегрального исчисления [Электронный ресурс]: учебное пособие / Г.М. Фихтенгольц - Издательство "Лань", 2020-2021. Т. 1-3. - Режим доступа: <https://e.lanbook.com/book/147144> , <https://e.lanbook.com/book/159505> , <https://e.lanbook.com/book/149365> .
2. Демидович Б.П. Сборник задач и упражнений по математическому анализу [Электронный ресурс]: учебное пособие / Б.П. Демидович - Издательство "Лань", 2021. 624 с. - Режим доступа: <https://e.lanbook.com/book/153688> .
3. Огнева Э. Н. Математика: Раздел 1. Алгебра и геометрия : учебное пособие / Э. Н. Огнева/ - Кемерово : Кемеровский государственный университет культуры и искусств (КемГУКИ), 2011. - 227 с. : табл., схем. - Режим доступа : <https://biblioclub.ru/index.php?page=book&id=227759>
4. Бортакровский А. С. Линейная алгебра и аналитическая геометрия. Практикум : учебное пособие / А. С. Бортакровский, А. В. Пантелеев; Московский авиационный институт (национальный исследовательский университет). - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2023. - 352 с. - (Высшее образование: Бакалавриат). - ВО - Бакалавриат. – Режим доступа: <https://znanium.com/catalog/document?id=432197>
5. Жукова Г. С. Аналитическая геометрия. Векторная и линейная алгебра: учебное пособие / Г.С. Жукова, М.Ф. Рушайло. — Москва : ИНФРА-М, 2019. — 415 с. — (Высшее образование). – Электронный ресурс. – Режим доступа: <https://znanium.com/catalog/document?id=352246>
6. Клетеник, Д. В. Сборник задач по аналитической геометрии : учебное пособие / Д. В. Клетеник ; под редакцией Н. В. Ефимова. — 17-е изд., стер. — Санкт-Петербург : Лань, 2020. — 224 с. — (Профессиональное образование). — Электронный ресурс. — Режим доступа: <https://e.lanbook.com/book/130489>
7. Шевелев, Ю.П. Дискретная математика. [Электронный ресурс] — Электрон. дан. — СПб.: Лань, 2016. — 592 с. — Режим доступа: <http://e.lanbook.com/book/71772>
8. Пятаева А. В. Интеллектуальные системы и технологии [Электронный ресурс] : учебное пособие / А. В. Пятаева, К. В. Раевич; Пятаева А. В., Раевич К. В. - Красноярск : СФУ, 2018. - 144 с. - Книга из коллекции СФУ - Информатика. – Режим доступа: <https://e.lanbook.com/book/157576>
9. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин; Московский институт электронной техники. - 1. - Москва : Издательский Дом "ФОРУМ", 2023. - 416 с. – Режим доступа : <https://znanium.com/catalog/document?id=418929>.

10. Сычев Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю. Н. Сычев; Российский экономический университет им. Г.В. Плеханова. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2023. - 201 с. - (Высшее образование: Магистратура). - ВО - Бакалавриат. -Режим доступа: <https://znanium.com/catalog/document?id=420080>
11. Сергеева, Ю.С. Защита информации: Конспект лекций: учебное пособие / Ю.С. Сергеева. - М. : А-Приор, 2011. - 128 с. - (Конспект лекций). - ISBN 978-5-384-00397-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=72670>
12. Зыков, Р. И. Системы управления базами данных [Электронный ресурс] / Р. И. Зыков. – М.: Лаборатория книги, 2012. – 162 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=142314>
13. Горожанина Е. И. Проектирование баз данных и баз знаний [Электронный ресурс] : учебное пособие / Е. И. Горожанина; Горожанина Е. И. - Самара : ПГУТИ, 2021. - 108 с. - Книга из коллекции ПГУТИ –Режим доступа: <https://e.lanbook.com/book/301085>
14. 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>
15. 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>
16. Кутликова И. В. Представление и кодирование информации. Логические основы обработки информации [Электронный ресурс] : учебно-методическое пособие / И. В. Кутликова, И. А. Черенкова, М. В. Новиков. - Москва : МГАВМиБ им. К.И. Скрябина, 2022. - 99 с. – Режим доступа: <https://e.lanbook.com/book/331364>
17. Сидельников, В. М. Теория кодирования [Электронный ресурс] / В. М. Сидельников. - М.: ФИЗМАТЛИТ, 2008. - 324 с. - ISBN 978-5-9221-0943-7 [Электронный ресурс]. – Режим доступа: <http://znanium.com/go.php?id=544713>

18. Чуканов С. Н. Теория информации [Электронный ресурс] : учебное пособие / С. Н. Чуканов. - Омск : ОмГТУ, 2022. - 192 с. - Книга из коллекции ОмГТУ - Информатика. Режим доступа: <https://e.lanbook.com/book/343790>
19. Попов, И. Ю. Теория информации : учебник для вузов / И. Ю. Попов, И. В. Блинова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 160 с. — ISBN 978-5-8114-8338-9. — Текст: электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/175153>
20. Трухин, М. П. Моделирование сигналов и систем. Дифференциальные, дискретные и цифровые модели динамических систем : учебное пособие / М. П. Трухин ; под научной редакцией С. В. Поршнева. — Санкт-Петербург : Лань, 2022. — 228 с. — ISBN 978-5-8114-3792-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/206774>
21. Гуц А.К. Теория игр и защита компьютерных систем [Электронный ресурс]: учебное пособие/ А.К. Гуц, Т.В. Вахний.— Электрон. текстовые данные.— Омск: Омский государственный университет им. Ф.М. Достоевского, 2013.— 160 с.— Режим доступа: <http://www.iprbookshop.ru/24947.html>
22. Челноков, А. Ю. Теория игр : учебник и практикум для вузов / А. Ю. Челноков. — Москва : Издательство Юрайт, 2021. — 223 с. — (Высшее образование). — ISBN 978-5-534-00233-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469214>
23. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — 2-е изд. — Саратов : Профобразование, 2019. — 446 с. — ISBN 978-5-4488-0091-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/87998.html>
24. Лапони́на, О.Р. Криптографические основы безопасности / О.Р. Лапони́на. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=429092>
25. Ракитин, Р. Ю. Компьютерные сети : учебное пособие / Р. Ю. Ракитин, Е. В. Москаленко. — Барнаул : АлтГПУ, 2019. — 340 с. — ISBN 978-5-88210-942-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/139182>
26. Закон Российской Федерации « Об информации, информатизации и защите информации» Электронный ресурс]. - URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/)

27. Щербаков, А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие / А. Щербаков. – Москва : Книжный мир, 2009. – 352 с. – (Высшая школа). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=89798>
28. Губарь Ю.В. Введение в математическое моделирование : учебное пособие / Губарь Ю.В.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 178 с. — ISBN 978-5-4497-0865-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/101993.html>
29. Миронова, Л.И. Моделирование динамических процессов в существенно нелинейных системах : монография / Миронова Л.И., Кондратенко Л.А. — Москва : Русайнс, 2021. — 225 с. — ISBN 978-5-4365-6679-5. — URL: <https://book.ru/book/939949>.
30. Креопалов В. В. Технические средства и методы защиты информации : учебное пособие / В. В. Креопалов. - Технические средства и методы защиты информации. - Электрон. дан. (1 файл). - Москва : Евразийский открытый институт, 2011. - 278 с. – Режим доступа: <http://www.iprbookshop.ru/10871.html>