

**ФЕДЕРАЛЬНЫЙ ИНТЕРНЕТ-ЭКЗАМЕН ДЛЯ ВЫПУСКНИКОВ
БАКАЛАВРИАТА И СПЕЦИАЛИТЕТА (ФИЭБ)**

**НАПРАВЛЕНИЕ ПОДГОТОВКИ
09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА**

ПРИМЕРЫ ЗАДАНИЙ ПИМ

ЧАСТЬ 1 ПИМ

Дисциплина «Базы данных»

Задание (установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов)

Установите соответствие между основными терминами реляционной базы данных и их неформальными аналогами:

- 1) отношение
- 2) кортеж
- 3) атрибут

Варианты ответов:

- 1) количество столбцов в таблице
- 2) таблица
- 3) заголовок столбца таблицы
- 4) строка таблицы

Дисциплина «Безопасность жизнедеятельности»

Задание (укажите не менее двух вариантов ответов)

К **негативным** психофизиологическим факторам производственной среды относятся ...

Варианты ответов:

- 1) динамические перегрузки
- 2) биологические пестициды
- 3) монотонность труда
- 4) ионизирующие излучения

Дисциплина «Защита информации»

Задание (установите правильную последовательность в предложенной совокупности ответов)

Установите последовательность разделов документа «Доктрина информационной безопасности Российской Федерации».

Варианты ответов:

- 1) Организационная основа системы обеспечения информационной безопасности РФ
- 2) Информационная безопасность РФ
- 3) Основные положения государственной политики обеспечения информационной безопасности РФ и первоочередные мероприятия по ее реализации
- 4) Методы обеспечения информационной безопасности РФ

Дисциплина «Инженерная и компьютерная графика»

Задание (введите ответ в поле)

Плоская фигура проецируется в натуральную величину без искажения, если она _____ плоскости проекций.

Введите ответ

Дисциплина «Метрология, стандартизация и сертификация»

Задание (укажите не менее двух вариантов ответов)

Правовой основой обеспечения единства измерений является государственная система обеспечения единства измерений (ГСИ), которая включает ...

Варианты ответов:

- 1) основополагающие стандарты, устанавливающие общие требования, правила и нормы
- 2) методические указания и рекомендации
- 3) методики выполнения измерений
- 4) правила по метрологии

Дисциплина «Операционные системы»

Задание (установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов)

Установите соответствие между классами прерываний и перечисленными событиями:

- 1) внешнее прерывание
- 2) внутреннее прерывание
- 3) программное прерывание

Варианты ответов:

- 1) выполнение особой команды прерывания
- 2) создание процесса или потока
- 3) сигнал от таймера при завершении кванта процессорного времени
- 4) попытка деления на ноль или нарушение адресации

Дисциплина «Программирование»

Задание (введите ответ в поле)

Очередь хранится в циклическом векторе (за последним элементом следует первый). Указатель начала очереди равен индексу первого элемента, указатель конца – индексу свободного места за последним элементом. Очередь содержит целые числа:

индексы	0	1	2	3	4	5	6	7	8	9
значения	15	21	13	40	25	11	10	15	24	6

Указатель начала очереди равен 3, указатель конца очереди равен 7.

Количество элементов в очереди равно ...

Введите ответ

Дисциплина «Сети и телекоммуникации»

Задание (укажите не менее двух вариантов ответов)

Метод коммутации пакетов реализован в сетевых технологиях ...

Варианты ответов:

- 1) Frame Relay
- 2) SDH
- 3) ATM
- 4) ISDN

Дисциплина «ЭВМ и периферийные устройства»

Задание (введите ответ в поле)

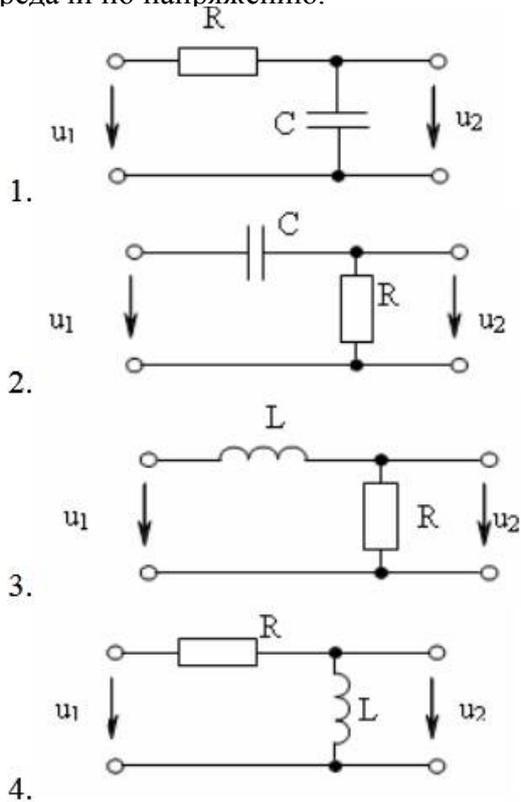
В микропроцессоре Intel физический адрес в реальном режиме вычисляется в блоке ...

Введите ответ

Дисциплина «Электротехника, электроника и схемотехника»

Задание (установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов)

Установите соответствие между схемой цепи и ее частотной характеристикой коэффициента передачи по напряжению.



Варианты ответов:

$$1) K_u(j\omega) = \frac{\dot{U}_{2m}}{\dot{U}_{1m}} = \frac{1}{1 + j\omega\tau}, \text{ где } \tau = RC$$

$$2) K_u(j\omega) = \frac{\dot{U}_{2m}}{\dot{U}_{1m}} = \frac{j\omega\tau}{1 + j\omega\tau}, \text{ где } \tau = R/L$$

$$3) K_u(j\omega) = \frac{\dot{U}_{2m}}{\dot{U}_{1m}} = \frac{j\omega\tau}{1 + j\omega\tau}, \text{ где } \tau = RC$$

$$4) K_u(j\omega) = \frac{\dot{U}_{2m}}{\dot{U}_{1m}} = \frac{1}{1 + j\omega\tau}, \text{ где } \tau = L/R$$

$$5) K_u(j\omega) = \frac{\dot{U}_{2m}}{\dot{U}_{1m}} = \frac{j\omega\tau}{1 + j\omega\tau}, \text{ где } \tau = L/R$$

ЧАСТЬ 2 ПИМ

Кейс-задание

(Тип задач профессиональной деятельности: научно-исследовательский)

Задание

На основе математического моделирования проигрываются различные сценарии кибератак и механизмы защиты от них в информационно-социальных системах, оценивается стойкость различных видов политики безопасности с возможностью вариации исходных параметров: топология и конфигурация системы защиты, структура и конфигурация команд кибератаки, методов, алгоритмов и средств реализации кибератак и защиты. Предполагается использовать методы планирования вычислительного эксперимента, методы математического программирования, методы компьютерного моделирования и анализа данных, имитационного моделирования, принятия решений, методы проведения измерений и наблюдений, исследований операций и др.

Злоумышленник средствами информационно-социальной системы «Одногруппники» пытается сформировать группу сообщников, пропагандирующих экстремистские взгляды и направления.

Краткое содержание информации	Имя файла	Скачать файл	
Базовые понятия теории вероятностей и математической статистики	k3_Pril1	PDF	DOC
Подсистемы парольной аутентификации пользователей. Оценка степени стойкости парольной защиты	k3_Pril2	PDF	DOC

Подзадача 1 (укажите не менее двух вариантов ответов)

В ходе моделирования процесса формирования злоумышленником группы сообщников, пропагандирующих экстремистские взгляды и направления, используется аппарат сетей Петри.

Формализация процесса моделирования возможна с помощью ...

Варианты ответов:

- 1) раскрашенной сети Петри
- 2) кольцевой сети Петри
- 3) стохастической сети Петри
- 4) временной сети Петри
- 5) многосвязной сети Петри
- 6) функциональной сети Петри

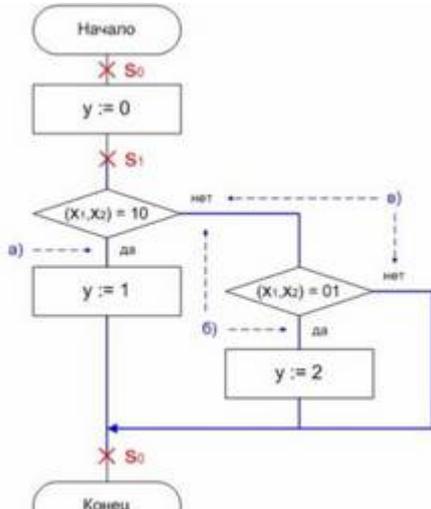
Подзадача 2 (установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов)

При моделировании процесса формирования злоумышленником группы сообщников в информационно-социальной системе «Одногруппники», пропагандирующих экстремистские взгляды и направления, используется теория автоматов.

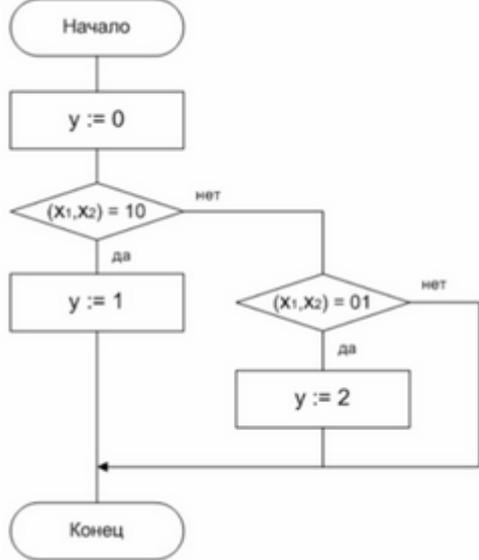
Установите соответствие между понятиями теории автоматов и их графической интерпретацией.

1. Автомат Мили
2. Автомат Мура
3. Граф переходов автомата Мили
4. Граф переходов автомата Мура

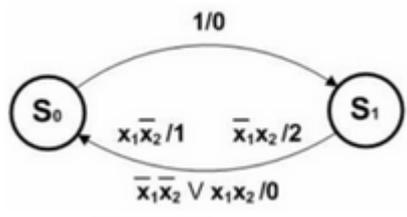
Варианты ответов:



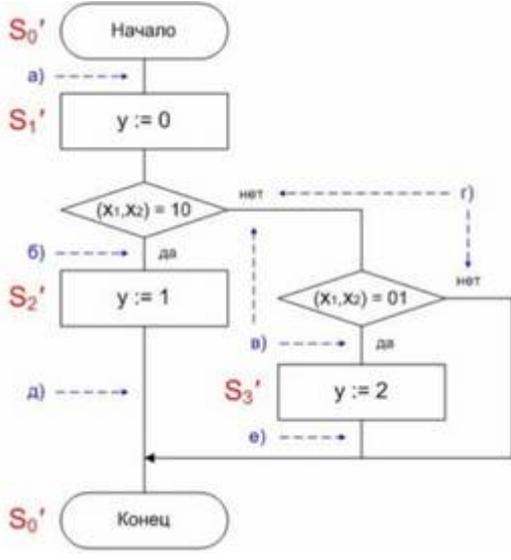
1)



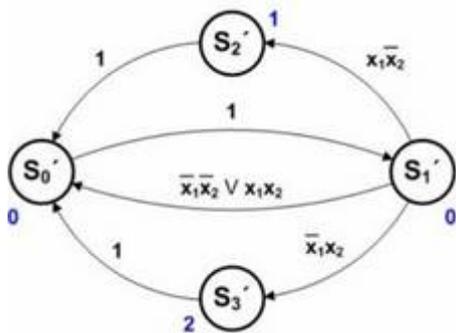
2)



3)



4)



5)

Подзадача 3 (установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов)

Известно, что на информационно-социальную систему «Одногруппники» случайным образом совершаются атаки.

Установите соответствие между статистическими показателями и их математическими формулами.

1. Математическое ожидание дискретной случайной величины
2. Математическое ожидание непрерывной случайной величины
3. Дисперсия случайной величины
4. Выборочная дисперсия

Варианты ответов:

- 1) $M(x) = \int x \cdot f(x) \cdot dx$
- 2) $D(x) = \frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^2$
- 3) $M(x) = \sum_{i=1}^n x_i \cdot p_i$
- 4) $D(x) = \frac{1}{n^2} \sum_{i=2}^n (x_i - \bar{x})^2$
- 5) $D(x) = M(x - m_x)^2$

Подзадача 4 (введите ответы)

Специалисты по информационной безопасности проанализировали сценарии кибератак и механизмы защиты от них в информационно-социальной системе. Выявлено, что сценарии кибератак характеризуются дискретной случайной величиной X , которая задана следующим законом распределения вероятностей:

X	1	3	4	5	7
p	0,2	?	0,1	0,3	0,2

Вычислить числовые характеристики X .

При решении задания используйте файл k3_Prill.

вероятность того, что случайная величина X примет значение 3

математическое ожидание случайной величины X

дисперсия случайной величины X (ответ округлите до сотых)

среднее квадратическое отклонение случайной величины X (ответ округлите до сотых)

Подзадача 5 (установите соответствие между нумерованными объектами в формулировке задания и вариантами ответов)

Злоумышленники в информационно-социальной системе «Одногруппники» используют криптографически защищенную децентрализованную платформу для анонимного общения и файлообмена «Retrosnare» с целью формирования группы сообщников, пропагандирующих экстремистские взгляды и направления.

Установите соответствие между терминами и их значениями.

1. Антитерроризм
2. Борьба с терроризмом
3. Анализ угрозы
4. Сдерживание

Варианты ответов:

- 1) меры предотвращения каких-либо действий при помощи внушения страха последствий данных действий
- 2) анализ уязвимости объекта с точки зрения совершения теракта с целью вскрытия и устранения слабых сторон в системе безопасности объекта
- 3) действия анти- и контртеррористического характера
- 4) меры безопасности, предпринятые с целью отбить у террористов намерение совершить теракт
- 5) защитные меры, используемые для снижения как уязвимости отдельных лиц, так и акций терроризма

Подзадача 6 (введите ответы)

Злоумышленник пытается взломать пароли пользователей.

В системе при составлении пароля пользователя можно использовать алфавит A , состоящий из строчных и заглавных букв латинского алфавита (латинский алфавит состоит из 26 символов) и цифр; срок действия пароля $T = 30$ дней; скорость перебора паролей злоумышленником $V = 15$ паролей в минуту.

Минимальная длина пароля L , при которой вероятность подбора пароля $P \leq 10^{-5}$, равна ...

При решении задания используйте файл k3_Pril2.

количество символов в алфавите

нижняя граница числа всевозможных паролей S^*

длина пароля L

количество всевозможных паролей S

**Базовые понятия теории вероятностей и
математической статистики**

Случайная величина характеризуется тем, что под воздействием случайных факторов она может с определенными вероятностями принимать те или иные значения из некоторого множества чисел. Случайная величина называется *дискретной*, если она принимает отдельные, изолированные друг от друга значения, и *непрерывной*, если множество ее значений непрерывно заполняет некоторый числовой промежуток.

Дискретную случайную величину, число возможных значений которой конечно, обычно представляют в виде ряда распределения, состоящего из пары чисел, одно из которых – значение величины, другое – вероятность появления этого значения, при этом сумма вероятностей появления всех значений равна 1.

Характеристикой непрерывной случайной величины является функция распределения, указывающая вероятность того, что эта случайная величина принимает значение, меньше заданной величины. Всему диапазону изменения случайной величины соответствует единичное значение функции распределения.

К основным числовым характеристикам случайных величин относятся математическое ожидание (наиболее вероятное ожидаемое значение), дисперсия (вариация) и среднее квадратическое отклонение.

Математическим ожиданием дискретной случайной величины называется сумма произведений всех ее значений на соответствующие вероятности

$$M(X) = \sum_{i=1}^n x_i \cdot p_i,$$

где $M(X)$ – математическое ожидание случайной величины X ;

x_i – i -е значение случайной величины X ;

p_i – вероятность появления i -го значения случайной величины X ;

i – порядковый номер дискретного значения случайной величины X ;

n – общее число дискретных значений случайной величины X .

Математическим ожиданием непрерывной случайной величины называется интеграл

$$M(X) = \int x \cdot f(x) \cdot dx,$$

где $f(x)$ – плотность распределения случайной величины X , представляющая собой производную по x функции распределения случайной величины X ;

\int – интеграл, который берется на всем интервале, в котором определена случайная величина X ;

dx – дифференциал случайной величины X .

Для большого числа случайных величин предполагается нормальное или близкое к нему распределение. Для случайной величины, имеющей нормальное распределение, математическое ожидание равно среднему значению генеральной совокупности.

Теоретическая (генеральная) дисперсия случайной величины определяется как математическое ожидание квадрата отклонения случайной величины X относительно ее математического ожидания:

$$D(X) = M(x - m_x)^2.$$

Дисперсию можно вычислить по формуле $D(X) = M(X^2) - (M(X))^2$.

Среднеквадратическое отклонение случайной величины X , характеризующее степень отклонения в среднем случайной величины в совокупности от своего среднего значения, представляет собой корень квадратный из ее дисперсии:

$$\sigma_x = \sqrt{D(X)}.$$

Данные о случайных величинах обычно представляются ограниченной выборкой, математическое ожидание которой оценивается *выборочной средней*, то есть *средним арифметическим значений случайной величины* в выборке

$$\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i,$$

где \bar{x} – выборочная средняя,

x_i – i -е значение случайной величины X ,

i – порядковый номер выборочного значения случайной величины X ,

n – общее число данных в выборке.

В статистическом исследовании очень часто бывает необходимо не только изучить вариации признака по всей совокупности, но и проследить количественные изменения признака по однородным группам совокупности, а также и между группами. Следовательно, помимо общей средней для всей совокупности необходимо просчитывать и частные средние величины по отдельным группам.

Различают дисперсии:

- общая;
- внутригрупповая;
- средняя внутригрупповая;
- межгрупповая.

Средняя внутригрупповая дисперсия свидетельствует о случайной вариации, которая может возникнуть под влиянием каких-либо неучтенных факторов и которая не зависит от признака-фактора, положенного в основу группировки. Данная дисперсия рассчитывается следующим образом: сначала рассчитываются дисперсии по отдельным группам (*внутригрупповая дисперсия*)

$$\sigma_i^2 = \frac{\sum (x - \bar{x}_i)^2 * f}{\sum f};$$

затем рассчитывается средняя из внутригрупповых дисперсий

$$\sigma_i^{-2} = \frac{\sum \sigma_i^2 * n_i}{\sum n_i},$$

где n_i – число единиц в группе.

Распределение Пуассона – вероятностное распределение дискретного типа, моделирует случайную величину, представляющую собой число событий, произошедших за фиксированное время, при условии, что данные события происходят с некоторой фиксированной средней интенсивностью и независимо друг от друга.

Асимптотическая формула Пуассона:

$$P_n(X = k) = \frac{\lambda^k}{k!} e^{-\lambda}$$

где $\lambda = np$, $k!$ – факториал числа k , $e = 2,718281828\dots$

Биномиальное распределение – дискретное распределение вероятностей случайной величины X , принимающей целочисленные значения $k = 0, 1, \dots, n$ с вероятностями:

$$P(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}.$$

Данное распределение характеризуется двумя параметрами:

целым числом $n > 0$, называемым *числом испытаний*, и вещественным числом p , $0 \leq p \leq 1$, называемом *вероятностью успеха в одном испытании*.

Биномиальное распределение – одно из основных распределений вероятностей, связанных с последовательностью независимых испытаний.

Если проводится серия из n независимых испытаний, в каждом из которых может произойти «успех» с вероятностью p , то случайная величина, равная числу успехов во всей серии, имеет указанное распределение. Эта величина также может быть представлена в виде суммы $X = X_1 + X_2 + \dots + X_n$ независимых слагаемых, имеющих распределение Бернулли.

Основные свойства биномиального распределения

Характеристическая функция: $\phi(t) = (1 + p(e^{it} - 1))^n$.

Моменты:

- Математическое ожидание: $M(X) = np$.
- Дисперсия: $D(X) = np(1 - p)$.
- Асимметрия: $\gamma_1 = \frac{1 - 2p}{\sqrt{np(1 - p)}}$; при $p = 0,5$ распределение симметрично относительно центра $n/2$.

Подсистемы парольной аутентификации пользователей.

Оценка степени стойкости парольной защиты

Под *идентификацией* пользователя понимают присвоение ему некоторого несекретного идентификатора, который он должен предъявить системе защиты информации (СЗИ) при осуществлении доступа к объекту. Под *аутентификацией* понимают подтверждение пользователем своего идентификатора, проверку его подлинности. Информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника с целью подобрать аутентифицирующую информацию (пароль) легального пользователя.

Некоторые из требований к выбору пароля и к подсистеме парольной аутентификации:

- пароль должен состоять из различных групп символов, и в нем не должны использоваться реальные слова, имена, фамилии, даты рождения и т. п.;
- администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего он должен быть сменен;
- в подсистеме парольной аутентификации должно быть установлено ограничение числа попыток ввода пароля.

Возможным методом взлома подсистемы парольной аутентификации является прямой перебор паролей.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля), например, если пароль состоит только из малых английских букв, то $A = 26$;

L – длина пароля;

$S = A^L$ – число всевозможных паролей длины L , которые можно составить из символов алфавита A ;

V – скорость перебора паролей злоумышленником (паролей в мин);

T – максимальный срок действия пароля (мин).

Тогда вероятность P подбора пароля злоумышленником в течение срока его действия V определяется по формуле

$$P = \frac{V * T}{S} = \frac{V * T}{A^L} \quad (1)$$

Эту формулу можно использовать для решения следующей задачи.

ЗАДАЧА. Определить минимальные мощность алфавита паролей A и длину паролей L , обеспечивающих вероятность подбора пароля злоумышленником не более заданной P , при скорости подбора паролей V , максимальном сроке действия пароля T .

При исходных данных V , T , P однозначно можно определить лишь нижнюю границу S^* числа всевозможных паролей по формуле

$$S^* = \frac{V * T}{P} \quad (2)$$

После нахождения нижней границы S^* необходимо выбрать такие A или L для формирования $S = A^L$, чтобы выполнялось неравенство (3).

$$S^* \leq S = A^L \quad (3)$$

При выборе S , удовлетворяющего неравенству (3), вероятность подбора пароля злоумышленника (при заданных значениях V и T) будет меньше, чем заданная P .