МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО
ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Воронежский государственный технический университет»

Кафедра радиотехники

# ТЕХНИЧЕСКАЯ ДИАГНОСТИКА И СКРЫТНОСТЬ

## МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к лабораторным работам
для студентов направления 11.04.01 «Радиотехника»
(магистерская программа «Радиотехнические средства
обработки и защиты информации в каналах связи»)

Воронеж 2025

УДК 621.396(07)
ББК 32.85я7

**Составитель**
*канд. техн. наук, доц. Р. П. Краснов*

**Техническая диагностика и скрытность:** методические указания к лабораторным работам для студентов направления 11.04.01 «Радиотехника» (магистерская программа «Радиотехнические средства обработки и защиты информации в каналах связи») / ФГБОУ ВО «Воронежский государственный технический университет»; сост. Р. П. Краснов. Воронеж: Изд-во ВГТУ, 2025. 34 с.

В методических указаниях приведены материалы для выполнения лабораторных работ по дисциплине «Техническая диагностика и скрытность». Представлены необходимые минимальные теоретические сведения и вопросы для самоподготовки.

Предназначены для студентов направления 11.04.01 «Радиотехника» (магистерская программа «Радиотехнические средства обработки и защиты информации в каналах связи»).

Подготовлены в электронном виде и содержатся в файле ЛР_ТД и С_2025.pdf.

Ил. 13. Табл.6. Библиогр.: 4 назв.

**УДК 621.396(07)**
**ББК 32.85я7**

**Рецензент** – А. В. Володько, канд. техн. наук, доцент кафедры радиоэлектронных устройств и систем ВГТУ

*Издается по решению редакционно-издательского совета Воронежского государственного технического университета*

## РАБОТА С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Для выполнения лабораторных работ используется ПО для исследования последовательного и дихотомического алгоритмов поиска, рабочее окно которого показано на рис. 1.

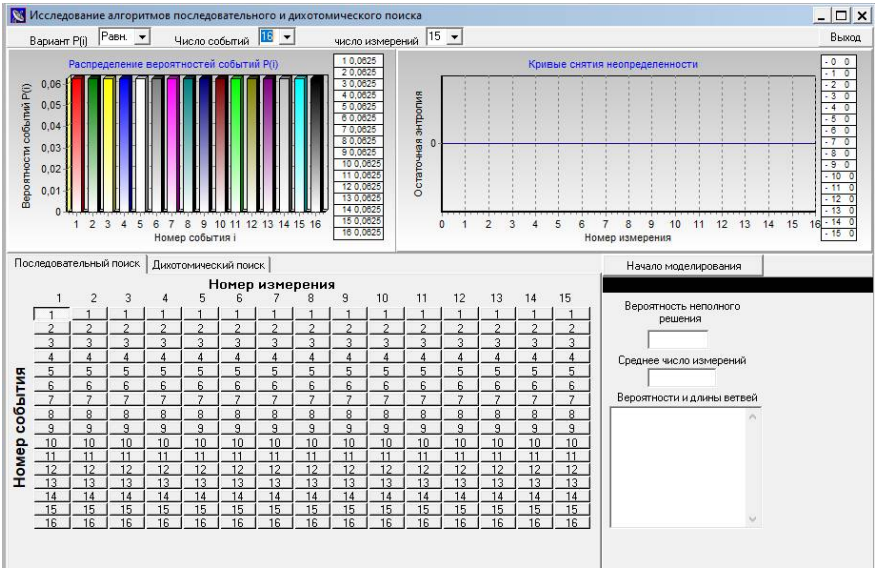


Рис. 1. Главное окно ПО

В верхней части окна имеются списки выбора распределения вероятностей (равномерное, экспоненциальное, либо определяемое вариантом от 1 до 15), числа событий $M$ (4, 8, 12, 16) и максимального числа измерений $N_{max}$ (от 1 до 15). Ниже в таблицах отображаются выбранное распределение вероятностей $P_m$ и кривая снятия неопределенности (КСН).

В поле поиска нажатием кнопок можно определять поисковый алгоритм – нажатая кнопка означает, что при данном измерении проверяется наличие соответствующего события. Последовательный поиск в каждом измерении проверяет одно событие, а дихотомический – любую группу событий.

Выбор поискового алгоритма осуществляется закладками в верхней части поля поиска.

На рис. 2 показано окно при выборе последовательного поиска для восьми событий ($M$ = 8) при равномерном законе распределения вероятностей.

После установки рабочих параметров и выбора алгоритма поиска, нажимается кнопка «Начало моделирования».

В такой конфигурации будет производиться последовательный перебор событий, начиная с первого (номер измерения $n$ равен номеру события $m$). Такой алгоритм будет неполным, так как не проверяются события с номерами 6, 7 и 8. Поэтому получаемая вероятность 0,375 не позволяет вынести решение, а КСН не достигает нуля. При этом на графике КСН пунктиром отображается потенциальная кривая, определяющее наименьшее значение КСН.

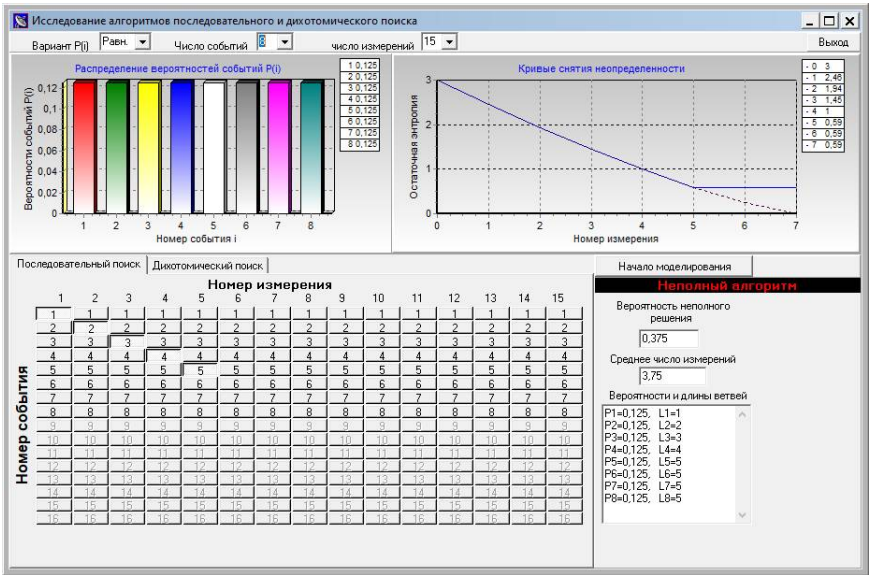


Рис. 2. Главное окно ПО при последовательном поиске

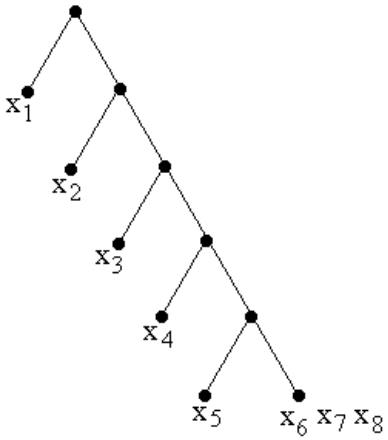


Рис. 3 Дерево поиска

Структура дерева поиска соответствует нажатым кнопкам, его параметры отображаются в правом нижнем окне. Показанной конфигурации соответствует дерево поиска, показанное на рис. 3.

Как видно, не проверяются события с номерами 6, 7 и 8. Если алгоритм поиска дополнить еще двумя измерениями, он станет полным, вероятность неполного решения станет равной нулю, а среднее число измерений увеличится.

ПО в режиме дихотомического поиска имеет вид, приведенный на рис. 4.

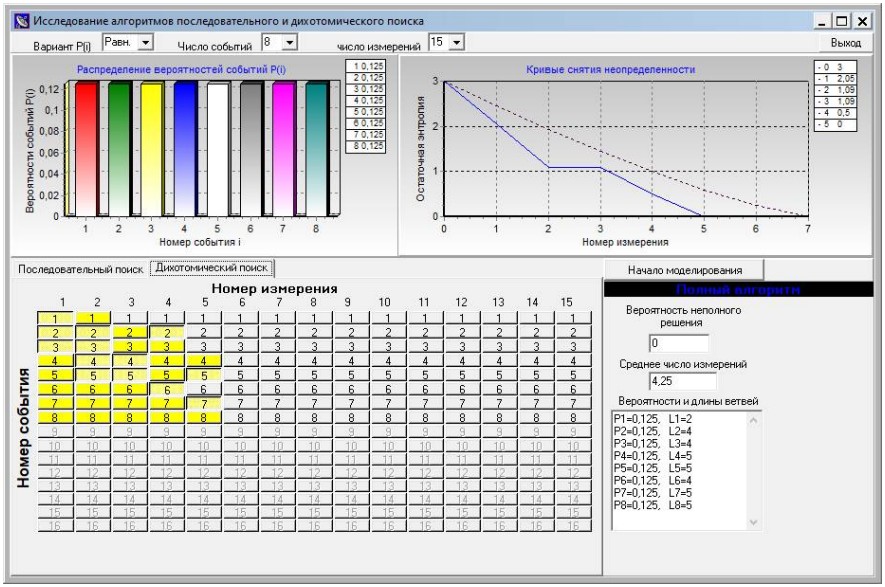


Рис. 4. Главное окно ПО в режиме дихотомического поиска

Желтым цветом показаны ветви дерева поиска. Если алгоритм неполный, то отметки желтым цветом нет, расчет характеристик поиска не производится и выдается сообщение «Неполный алгоритм».

Нажатым кнопкам наборного поля соответствует дерево поиска, приведенное на рис. 5.

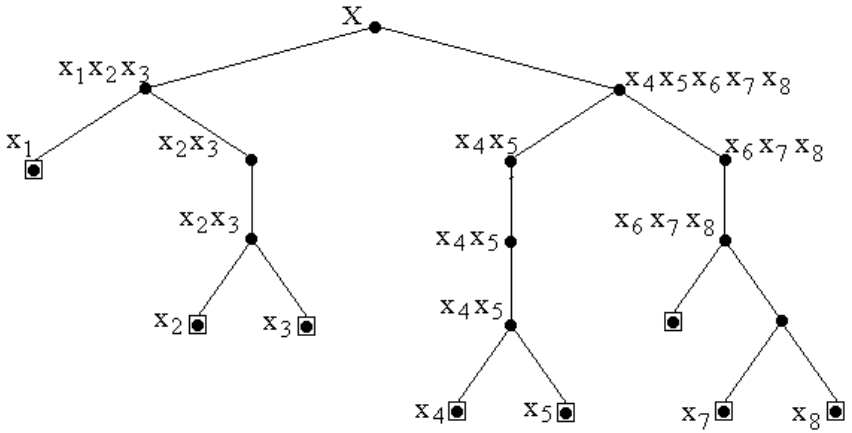


Рис. 5. Дерево поиска для рис. 4

В этом случае третье измерение получится полностью холостым, что и будет соответствовать горизонтальному участку на КСН.

При выборе распределения вероятностей по варианту (равен сумме последних двух цифр в зачетной книжке) следует иметь в виду, что текущее значение распределения формируется программой при каждом ее запуске. Следовательно, при повторном запуске это распределение будет меняться.

# ЛАБОРАТОРНАЯ РАБОТА № 1
# ОПРЕДЕЛЕНИЕ АЛГОРИТМИЧЕСКОЙ СКРЫТНОСТИ

*Цели работы*

1. Ознакомление с понятием скрытности.
2. Ознакомление с алгоритмами поиска.
3. Изучение принципов построения дерева поиска.

*Краткие теоретические сведения*

Поисковую процедуру можно представить графически в виде *дерева поиска*, состоящего из узлов (точек) и соединяющих их линий (ветвей), например, как показано на рис. 3.

Построение начинается с корневого узла в вершине дерева поиска. Узлы, в которых поиск заканчивается, называют *финальными*, они завершают ветви дерева поиска. Число финальных узлов равно $A$. Состав входящих в выбранное подмножество событий определяется финальными узлами, следующими вниз по дереву поиска.

Переход от одного узла к другому по дереву поиска сопровождается одним *двоичным измерением*, которое сокращенно обозначается ДИЗ.

*Длину пути* в диз'ах от корневища дерева $X$ к $i$-му финальному узлу $x_i$ будем обозначать через $l_i$. Вероятность реализации $i$-го пути при поиске $p(l_i)$ равна вероятности реализации соответствующего состояния объекта $P(l_i) = P(x_i) = P_i$.

Длина пути $l_i$ и его траектория зависят от алгоритма поиска, определяющего структуру дерева.

*Алгоритмической скрытностью* $R$ называется среднее число двоичных измерений, необходимых для выявления реасобытия при заданном алгоритме поиска. Оно равно средней длине ветвей $\bar{l}$ дерева поиска от корня к финальным узлам

$$R = M(l_i) = \sum_{i=1}^{A} P(l_i) l_i \ . \qquad (1)$$

Алгоритмическая скрытность характеризует средние затраты в диз'ах на выявление реасобытия при заданном алгоритме поиска. В определении (1) полагается, что ошибки

отсутствуют, и все измерения имеют единичную стоимость независимо от порядка их выполнения в процедуре поиска.

*Лабораторное задание*

1. В соответствии с вариантом задания выбрать из таблицы в приложении распределение вероятностей $P(x_i)$ состояний $x_i$, $i = 1…A$, построить его график.

2. Определить алгоритмическую скрытность $R_1$ состояний объекта для полного алгоритма поиска «$m = n$», при котором в ходе $n$-го измерения проверяется «$m = n$» - ое состояние (рис. 6, а). Полученное $R_1$ занести в табл. 1.

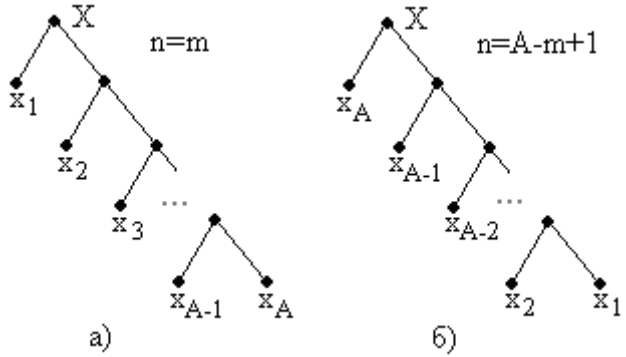


Рис. 6. Дерево последовательного поиска

Таблица 1

Значения алгоритмической скрытности

| $R_1$ | $R_2$ | $R_3$ | $R_4$ | $R_5$ | $R_6$ |
|---|---|---|---|---|---|
| | | | | | |

3. Повторить расчет для алгоритма поиска «$m=A-n+1$». В этом случае при $n$-ом измерении проверяется $m=(A-n+1)$-ое состояние (рис. 6, б). Полученное значение алгоритмической скрытности $R_2$ занести в табл. 1.

4. Повторить расчеты для равномерного распределения вероятностей и определить скрытности $R_3$ и $R_4$ для алгоритмов

на рис. 6, а и рис. 6, б соответственно. Результат занести в табл. 1.

5. Произвести расчет алгоритмической скрытности $R_5$ для распределения вероятностей $P(x_i)$ состояний $x_i$, $i = 1…A$, задав дихотомический алгоритм поиска. Примеры такого дерева приведены на рис. 7, а и рис. 7, б для $A = 2^2 = 4$ и $A = 5$ соответственно (дерево поиска следует построить для своего варианта задания). Полученное значение $R_5$ занести в табл. 1.

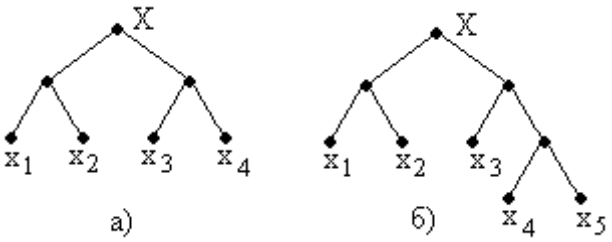


Рис. 7. Дерево поиска для дихотомического алгоритма

6. Повторить расчеты по п. 5 для равномерного распределения вероятностей, полученное значение алгоритмической скрытности $R_6$, занести в табл. 1.

7. В выводе сравнить и объяснить полученные результаты.

*Содержание отчета*

1. Название, цель работы.
2. График распределения вероятностей.
3. Данные измерений и результаты расчетов.
4. Краткие выводы по результатам работы.

*Вопросы для самопроверки*

1. Описание поисковой процедуры, модель двоичного поиска.
2. Дерево поиска, его свойства.
3. Виды алгоритмов поиска, примеры описания.
4. Кривая снятия неопределенности (КСН).
5. Алгоритмическая и потенциальная скрытность.

# ЛАБОРАТОРНАЯ РАБОТА № 2
# РАСЧЕТ ИНФОРМАЦИОННЫХ ХАРАКТЕРИСТИК ПОИСКА

*Цели работы*

1. Ознакомление с понятием скрытности.
2. Ознакомление с последовательными и дихотомическим алгоритмами поиска.
3. Изучение принципов построения дерева поиска.

*Краткие теоретические сведения*

Энтропия $H(X)$ является мерой исходной (априорной) неопределенности состояний объекта и определяется априорным распределением их вероятностей.

Если проведено первое двоичное измерение и принято решение $y_1$ о наличии реасобытия в одном из анализируемых подмножеств $X_0$ ($y_1 = 0$) или $X_1$ ($y_1 = 1$), то апостериорное распределение вероятностей $p(x_i|y_1)$ состояний $x_i$ объекта после первого измерения отличается от априорного $p_1$, а это приводит к изменению средней апостериорной неопределенности (энтропии), равной

$$H_1(X) = -\sum_{y_1=0}^{1} P(y_1) \sum_{i=1}^{A} p(x_i|y_1)\, log_2[\,p(x_i|y_1)],$$

где $P(y_1)$ - вероятность соответствующего решения $y_1$, а

$$H(X|y_1) = -\sum_{i=1}^{A} p(x_i|y_1)\, log_2[\,p(x_i|y_1)],$$

- условные апостериорные энтропии для соответствующих решений.

При безошибочном поиске энтропия снижается после каждого двоичного измерения. Для описания этого явления удобно использовать декремент неопределенности $\Delta H_n(X)$ после $n$-го измерения, равный разности средних априорной и апостериорной энтропий для этого измерения,

$$\Delta H_n(X) = H_{n-1}(X) - H_n(X).$$

Для безошибочного поиска частный (условный) декремент неопределенности в ходе $n$-го двоичного измерения при заданном наборе (векторе) $y_1$, $y_2$, …, $y_{n-1}$ ранее принятых решений можно определить по формуле

$$\Delta H_n(X|y_1, y_2, \dots, y_{n-1}) =$$
$$= -p(y_n = 0|y_1, y_2, \dots, y_{n-1}) \cdot log_2[\, p(y_n = 0)|y_1, y_2, \dots, y_{n-1}] -$$
$$-p(y_n = 1|y_1, y_2, \dots, y_{n-1}) \cdot log_2[\, p(y_n = 1|y_1, y_2, \dots, y_{n-1})],$$

где $p(y_n|y_1, y_2, \dots, y_{n-1})$ – условная вероятность принятия решения $y_n$. Можно использовать равенство

$$p(y_n = 0|y_1, y_2, \dots, y_{n-1}) + p(y_n = 1|y_1, y_2, \dots, y_{n-1}) = 1.$$

Обозначим

$$p(y_n = 0|y_1, y_2, \dots, y_{n-1}) = p,$$

тогда получим

$$\Delta H_n(X|y_1, y_2, \dots, y_{n-1}) = -p\, log_2\, p - (1 - p)\, log_2(\, 1 - p).$$

Нетрудно убедиться, что

$$\Delta H_n(X|y_1, y_2, \dots, y_{n-1}) \le 1,$$

то есть условный декремент неопределенности не может быть больше 1 бита. Это неравенство удобно для контроля правильности результатов расчета.

Средний (безусловный) декремент неопределенности равен

$$\Delta H_n(X) =$$
$$\sum_{y_1, y_2, \dots, y_{n-1}} p(y_1, y_2, \dots, y_{n-1}) \Delta H_n(X|y_1, y_2, \dots, y_{n-1}),$$

где $p(y_1, y_2, \dots, y_{n-1})$ – вероятность возникновения соответствующего вектора решений.

При безошибочном поиске для ветвей, длина которых меньше $n$, поиск завершен и соответствующая условная энтропия равна нулю.

*Лабораторное задание*

1. В соответствии с вариантом задания из приложения выбрать распределение вероятностей $P(x_i)$ состояний $x_i$, $i = 1 \dots A$, построить его график.

2. Провести расчет кривой снятия неопределенности (КСН) $H_1(n)$ для последовательного алгоритма поиска с деревом, показанным на рис. 6, а, построить дерево поиска и график КСН.

3. Провести расчет КСН $H_2(n)$ для дихотомического алгоритма поиска, приведенного на рис. 7. Изобразить дерево поиска в соответствии с заданным арсеналом множества состояний $A$. Построить график КСН.

4. Повторить расчеты п. 2 и 3 для выбора равномерного распределения вероятностей состояний. Построить полученные графики КСН $H_3(n)$ и $H_4(n)$.

5 Провести расчет значений декрементов неопределенности $\Delta H(n)$ для четырех полученных ранее КСН. По результатам расчетов построить соответствующие графики зависимостей.

6. В выводе сравнить и объяснить полученные результаты.

*Содержание отчета*

1. Название, цель работы.
2. График распределения вероятностей.
3. Данные измерений и результаты расчетов.
4. Графики полученных КСН.
5. Краткие выводы по результатам работы.

*Вопросы для самопроверки*

1. Неопределенность возможных состояний объекта, их энтропия
2. Количество информации в сообщении.
3. Количество информации в результате одного двоичного измерения, декремент неопределенности.
4. Связь между неопределенностью состояний (энтропией) и потенциальной скрытностью.
5. Баланс неопределенностей

## ЛАБОРАТОРНАЯ РАБОТА № 3
## ИССЛЕДОВАНИЕ АЛГОРИТМА ПОСЛЕДОВАТЕЛЬНОГО ПОИСКА

*Цели работы*

1. Ознакомление с понятием скрытности.
2. Ознакомление с последовательными алгоритмами поиска.
3. Изучение принципов построения дерева поиска.

*Краткие теоретические сведения*

При анализе структур данных, относящихся к поиску на множестве упорядоченных данных, процедуру поиска рассматривают изолированно. В этом случае при поиске некоторого элемента не учитываются результаты предыдущих операций поиска. Например, в двоичном дереве поиск элемента всегда начинается от корня, независимо от того, насколько близки результаты двух последовательных операций поиска.

Однако, если начинать поиск из элемента, в котором закончилась предыдущая операция поиска, то часто результата можно достичь быстрее.

Поиск, основанный на таких соображениях, будем называть «последовательным поиском».

*Лабораторное задание*

1. Установить равномерное распределение вероятностей событий при их числе $A = 8$ для четного и $A = 12$ для нечетного вариантов. Задать максимальное число измерений $n = 15$.

На наборном поле задать полный алгоритм поиска «$m = n$», при котором номер события $m$ равен номеру измерения $n$ (последнее событие не проверяется. Построить дерево поиска. Запустить моделирование, определить среднее число измерений $R_1$. Результат занести в табл. 2. Сделать скриншот с результатами работы, занести в отчет.

Таблица 2

| $R_1$ | $R_2$ | $R_3$ | $R_4$ | $R_5$ | $R_6$ | $R_7$ | $R_8$ | $R_9$ |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

2. На наборном поле включить проверку последнего события, построить дерево поиска, определить среднее число измерений $R_2$, занести его в табл. 2. Произвести расчет скрытностей $R_1$ и $R_2$.

3. Установить алгоритм поиска «$m = A\text{-}n+1$», при котором первым проверяется последнее событие, а последним – второе, построить дерево поиска. Определить среднее число измерений $R_3$, занести его в табл. 2.

4. Установить экспоненциальное распределение вероятностей событий вида $P_j = B \cdot 2^{-j}$, где $j = 1 \ldots A$, $B$ - нормирующий множитель. Параметр $A$ следует выбрать аналогичным п.1. Установить алгоритм поиска «$n = m$» без проверки последнего события.

Определить среднее число измерений $R_4$, занести его в табл. 2. Произвести расчет величины $R_4$.

5. Задать алгоритм поиска «$m = A\text{-}n+1$». По результатам моделирования найти среднее число измерений $R_5$, занести его в табл. 2. Произвести расчет величины $R_5$.

6. Выбрать распределение вероятностей в соответствии со своим вариантом задания при числе событий $A = 4$. Пример рабочего окна показан на рис. 8.

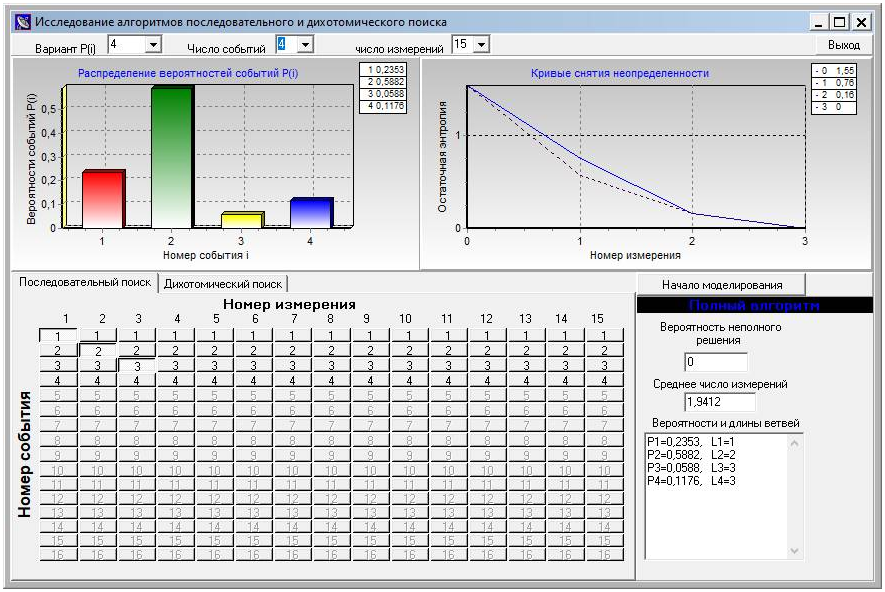


Рис. 8. Окно последовательного поиска

7. Задать алгоритм поиска «$n = m$» без проверки последнего события, выполнить моделирование. Сделать скриншот с результатами работы, сохранить в отчет. Среднее число измерений $R_6$ занести в табл. 2.

8. Повторить моделирование, аналогично п. 7 для числа событий $A$ = 8, 12 и 16. Полученные значения средних чисел измерений $R_7$, $R_8$ и $R_9$ занести в табл. 2. Провести сравнительный анализ результатов.

Все рассмотренные алгоритмы сопроводить соответствующими деревьями поиска.

*Содержание отчета*

1. Название, цель работы.
3. Данные измерений и результаты расчетов.
4. Деревья поиска для всех видов установок расчетов.
5. Краткие выводы по результатам работы.

*Вопросы для самопроверки*

1. Виды скрытностей.
2. Дерево поиска, его свойства.
3. Виды алгоритмов поиска, примеры описания.
4. Кривая снятия неопределенности (КСН).

## ЛАБОРАТОРНАЯ РАБОТА № 4
## ИССЛЕДОВАНИЕ ВЛИЯНИЯ РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ НА АЛГОРИТМИЧЕСКУЮ СКРЫТНОСТЬ

*Цели работы*

1. Ознакомление с понятием скрытности.
2. Ознакомление понятиями алгоритмической скрытности.
3. Изучение принципов построения дерева поиска.

*Краткие теоретические сведения*

На формирование оптимального алгоритма поиска и соответствующего ему дерева сильно влияют распределения вероятностей состояний объекта.

Рассмотрим закон распределения вероятностей состояний объекта в виде показательной функции $P_i = \beta 2^{-\lambda i}$, где $\lambda$ -

коэффициент затухания, $\beta$ - нормирующий множитель, $i = \overline{1, A}$. Так как сумма вероятностей равна единице, то величина $\beta$ в соответствии с выражением для суммы членов геометрической прогрессии будет равна

$$\beta = \frac{2^{\lambda}-1}{1-2^{-\lambda A}}.$$

При $\lambda \to 0$ получим равномерное распределение вероятностей $P_i = \beta = 1/A$, а иначе вероятности уменьшаются с ростом номера состояния.

Можно имитировать различные законы распределения вероятностей состояний объекта с разными значениями $\lambda$, $A$ и $\beta$.

При равновероятном распределении вероятностей состояний и их арсенале $A = 2^n$ ($n$ - целое число) потенциальная скрытность определяется $S = \log_2 A = n$ двоичных измерений.

Можно показать, что если параметр $\lambda$ удовлетворяет неравенству

$$\lambda > log_2 \left[\frac{1}{\sqrt{1{,}25}-0{,}5}\right] \approx 0{,}694,$$

то сумма вероятностей двух последних состояний меньше вероятности предшествующего состояния. Тогда в соответствии с методом Циммермана – Хаффмена оптимальным оказывается *последовательный* алгоритм поиска, а потенциальная скрытность определяется выражением

$$S = \sum_{i=1}^{A-1} \beta 2^{-\lambda i} i + (A-1)\beta 2^{-\lambda A}.$$

Если параметр $\lambda$ не удовлетворяет этому условию, то последовательный поиск не является оптимальным.

При выравнивании распределения вероятностей состояний объекта оптимальное дерево поиска трансформируется от последовательного до дихотомического.

*Лабораторное задание*

1. Рассчитать экспоненциальное распределение вероятностей $P_1(x_i)$, $i = 1\ldots A$. вида

$$P_1(x_i) = \frac{\exp(-\alpha \cdot i)}{\sum_{k=1}^{A} \exp(-\alpha \cdot k)},$$

приняв $A = 4 + N$ и $\alpha = \alpha_1 = N / (N{+}10)$, где $N$-сумма двух последних цифр номера зачетной книжки. Построить его график.

2. Рассчитать скрытность $R_1$ множества состояний для последовательного алгоритма поиска, дерево которого показано на рис. 6, а. Значение $R_1$ занести в табл.3.

Таблица 3

| $R_1$ | $R_2$ | $R_3$ | $R_4$ |
|---|---|---|---|
| | | | |

3. Определить КСН $H_1(n)$ для последовательного алгоритма поиска, построить ее график.

4. Изменить параметр распределения $\alpha = \alpha_2 = \alpha_1/2$ и повторить расчеты по п. 2 и 3. Соответствующее значение скрытности $R_2$ занести в табл. 3, построить график КСН $H_2(n)$. Сравнить полученные результаты, сделать вывод о характере влияния параметра $\alpha$ на скрытность и КСН, записать его в соответствующий раздел отчета.

5. Рассчитать равномерное распределение вероятностей вида $P_3(x_i) = 1/A$, $i = 1\ldots A$. Рассчитать скрытность $R_3$ множества состояний для последовательного алгоритма поиска. Результат занести в табл. 3. Определить КСН $H_3(n)$, построить ее график.

6. Рассчитать экспоненциальное распределение вероятностей $P_4(x_i)$, $i = 1\ldots A$, при $\alpha = \alpha_4 = -\alpha_1$, построить график. Рассчитать скрытность $R_4$ множества состояний для последовательного алгоритма поиска, занести ее значение в табл. 3. Определить КСН $H_4(n)$, построить ее график.

Провести сравнительный анализ полученных результатов, записать краткий вывод по итогам анализа.

*Содержание отчета*

1. Название, цель работы.
2. График распределения вероятностей.
3. Данные измерений и результаты расчетов.
4. Графики полученных КСН.
5. Краткие выводы по результатам работы.

*Вопросы для самопроверки*

1. Понятие оптимального алгоритма поиска.
2. Понятие потенциальной скрытности.
3. Параметры и виды распределения вероятностей.
4. Влияние вида распределения на алгоритм поиска и скрытность.

## ЛАБОРАТОРНАЯ РАБОТА № 5
## ИССЛЕДОВАНИЕ ДИХОТОМИЧЕСКОГО АЛГОРИТМА ПОИСКА

*Цели работы*

1. Ознакомление с понятием скрытности.
2. Ознакомление с дихотомическими алгоритмами поиска.
3. Изучение принципов построения дерева поиска.

*Лабораторное задание*

1. Установить число событий $A = 8$ для четного варианта и $A = 16$ для нечетного при равномерном распределении вероятностей и число измерений $n = 15$. Временно включить режим последовательного поиска при алгоритме «$n = m$», провести моделирование.

Переключиться в режим дихотомического поиска. В правой верхней части экрана останется график КСН последовательного поиска (пунктир).

Построить дерево дихотомического поиска, задав его с помощью наборного поля, выполнить моделирование. Скриншот занести в отчет. Проанализировать графики КСН для дихотомического и последовательного алгоритмов поиска.

2. Установить число событий $A = 12$ и число измерений $n = 15$. Временно включить режим последовательного поиска при алгоритме «$n = m$», провести моделирование и переключиться в режим дихотомического поиска. Задать с помощью наборного поля дихотомический алгоритм поиска, провести моделирование, скриншот занести в отчет.

Рассчитать КСН для рассматриваемого случая, сравнить с результатами моделирования.

3. Выбрать экспоненциальное распределение вероятностей событий вида $P_j = B \cdot 2^{-j}$, где $j = 1 \ldots A$, $B$ - нормирующий множитель, при том же $A$, что и в п. 1. Задать дихотомический алгоритм поиска для этого случая. Провести моделирование, проанализировать результаты.

4. Выбрать распределение вероятностей событий в соответствии с суммой двух последних цифр номера зачетной книжки при $A = 8$. На наборном поле установить алгоритм дихотомического поиска. Провести моделирование, скриншот сохранить в отчет.

5. Задать алгоритм последовательного поиска «$n = m$», выполнить моделирование, скриншот сохранить в отчет. Проанализировать полученные результаты, сравнить КСН рассмотренных алгоритмов поиска.

Рассчитать КСН для алгоритмов дихотомического и последовательного поиска, сравнить их с результатами моделирования.

*Содержание отчета*

1. Название, цель работы.
2. Скриншоты для различного вида деревьев поиска.
3. Данные измерений и результаты расчетов.
4. Краткие выводы по результатам работы.

*Вопросы для самопроверки*

1. Описание поисковой процедуры, модель двоичного поиска.
2. Дерево поиска, его свойства.
3. Виды алгоритмов поиска, примеры описания.
4. Кривая снятия неопределенности (КСН).

# ЛАБОРАТОРНАЯ РАБОТА № 6
# ИЗУЧЕНИЕ МЕТОДОВ ОПТИМИЗАЦИИ ПОИСКА

*Цели работы*

1. Ознакомление с понятием скрытности.
2. Изучение методов оптимизации поиска.
3. Изучение методов безызбыточного кодирования.

*Метод Шеннона-Фано*

Исходное множество элементов сообщения (состояний объекта) с заданным распределением их вероятностей разбивается на два подмножества с номерами 0 и 1 так, чтобы вероятности попадания в них были максимально близки (равны 0,5). Затем каждое из полученных подмножеств отдельно разбивается на два подмножества с тем же условием и номерами соответственно 00, 01 и 10, 11. Разбиение заканчивается, когда все подмножества будут иметь только по одному элементу.

Как видно, все разбиения обеспечивают примерное равенство условных вероятностей появления реасобытия в каждом из подмножеств.

Оптимальность кода Шеннона-Фано обусловлена рациональным сочетанием длин ветвей дерева поиска с частостью употребления состояний объекта и последовательным делением множества $X$ на равновероятные подмножества с максимумом получения информации при каждом измерении. Выполняется иерархический принцип сочетания $P_i$ и $l_i$.

Среднее число двоичных измерений равно

$$R = \sum_{i=1}^{A} P_i l_i$$

Энтропия множества $X$ определяется выражением

$$H(X) = -\sum_{i=1}^{A} P_i \log P_i$$

*Метод Циммермана – Хаффмена*

Процедура оптимизации поиска по методу Циммермана-Хаффмена разделяется на два этапа, которые условно назовем «Заготовительные операции» и «Считывание».

Заготовительная операция состоит в ранжировании некоторого заданного множества состояний объекта $X$ по значениям их вероятностей.

Затем выполняется отделение двух последних элементов столбца $P$, имеющих наименьшие вероятности, и объединении их в один приведенный элемент путем сложения значений их вероятностей. При такого рода объединении двух наименее вероятных элементов самый нижний элемент помечается символом «1», следующий за ним – символом «0». Далее, приведенный элемент (помещен в прямоугольную рамку) вносится во второе ранжируемое множество в соответствии с его рангом вместе с другими оставшимися элементами из первого ранжированного множества. При ранжировании в первую очередь учитываются все элементы предшествующего множества, а затем – приведенные. Очевидно, что число элементов в новом ранжированном множестве на единицу меньше, чем в предыдущем. Сумма вероятностей в столбце $P$ остается по-прежнему равной 1.

Так продолжается до тех пор, пока в последнем ранжируемом столбце не останется только два элемента с выходом на букву $X$ в конце. Число ранжируемых столбцов на единицу меньше арсенала состояний $A$.

Считывание осуществляется в противоположном направлении от $X$ к возможным состояниям объекта $x_i$. Перемещаясь от последних символов «0» или «1» поочередно навстречу стрелкам, записываются все встретившиеся двоичные символы, результат представляется в виде таблицы кодирования состояний.

Экономичность кодов типа Циммермана-Хаффмена или Шеннона-Фано в отношении затрачиваемого числа двоичных символов на передачу текста или среднего числа диз при

раскрытии состояния объекта связана с равным или приближенно равным делением по вероятности на подмножества при измерениях. При этом декремент неопределенности при каждом измерении является максимальным.

*Лабораторное задание*

1. Для своего варианта задания (суммы двух последних цифр номера зачетной книжки) выбрать из таблицы в приложении распределение вероятностей $P(x_i)$ состояний $x_i$, $i = 1…A$, построить его график.

2. Для заданного распределения вероятностей разработать оптимальный алгоритм поиска с помощью метода Шеннона-Фано, построить дерево поиска. В отчете привести промежуточные результаты.

Рассчитать потенциальную скрытность состояний $S_1$ и КСН $H_1(n)$ для этого алгоритма, построить график КСН и значений декрементов неопределенности $\Delta H_1(n)$. Результаты расчетов занести в табл. 4.

3. Разработать оптимальный алгоритм поиска с помощью метода Циммермана-Хаффмена, построить дерево поиска. В отчете привести промежуточные результаты.

Рассчитать потенциальную скрытность $S_2$ состояний и КСН $H_2(n)$ для этого алгоритма, построить график КСН и значений декрементов неопределенности $\Delta H_2(n)$. Результаты расчетов занести в табл. 4.

4. Разработать оптимальные алгоритмы поиска с помощью методов Шеннона-Фано и Циммермана-Хаффмена для равномерного распределения вероятностей $P(x_i) = 1/A$, $i = 1…A$. Построить деревья поиска и рассчитайте значения потенциальной скрытности $S_3$ и $S_4$ для полученных алгоритмов.

Результаты расчетов занести в табл. 4.

Таблица 4

| $S_1$ | $S_2$ | $S_3$ | $S_4$ |
|---|---|---|---|
| | | | |

*Содержание отчета*

1. Название, цель работы.
2. График распределения вероятностей.
3. Данные измерений и результаты расчетов.
4. Графики полученных КСН.
5. Краткие выводы по результатам работы.

*Вопросы для самопроверки*

1. Минимальное среднее число двоичных измерений.
2. Оптимизация поиска на основе методов безызбыточного кодирования сообщений.
3. Двоичное кодирование.
4. Метод Шеннона-Фано.
5. Метод Циммермана – Хаффмена.

## ЛАБОРАТОРНАЯ РАБОТА № 7
## ИЗУЧЕНИЕ ОПТИМИЗАЦИИ АЛГОРИТМОВ ПОИСКА

*Цели работы*

1. Ознакомление с методами поисковых процедур.
2. Ознакомление методами оптимизации алгоритмов.
3. Изучение принципов построения дерева поиска.

*Краткие теоретические сведения*

Рассмотрим два примера оптимизации при разных законах распределения вероятностей состояний объекта с одновременным построением оптимальных поисковых деревьев.

*Оптимизация при усеченном показательном законе распределения вероятностей состояний.*

Представим показательный закон распределения вероятностей состояний объекта в виде:

$$P(x_i) = f(i) = \beta \cdot 2^{-\alpha \cdot i},$$

где $i$ - целочисленная независимая переменная (номер состояния), $i$ = 1, 2, …, $A$, где $A$ – арсенал возможных

состояний исследуемого объекта, $\alpha$ - показатель затухания функции с возрастанием $i$. Примем для расчетов $\alpha$ = 1, $\beta$ - нормирующий множитель, который вводится для обеспечения выполнения условия нормировки в соответствии с общим требованием $\sum_{i=1}^{A} \beta \cdot 2^{-i} = 1$, откуда $\beta = \frac{1}{\sum_{i=1}^{A} 2^{-i}}$.

Усеченным называется закон распределения при ограниченном $A$ ($A < \infty$).

С возрастанием $A$ значение $\beta$ стремится к 1 и $\alpha = 1$.

Примем следующее приближение: $P(i) = 2^{-i}$.

Представим *первое* измерение в виде развилки (рис. 9) с пометкой вверху $X$, что имеет отношение ко всему, нетронутому до поиска, множеству $X$ возможных состояний исследуемого объекта.

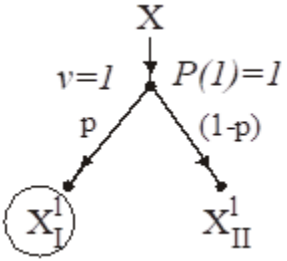


Рис. 9. Дерево первого измерения

Обозначим два нижних подмножества, на которые делится $X$ перед первым шагом поиска через $X_I^{\nu}$ и $X_{II}^{\nu}$. Вероятность первого шага вне зависимости от распределения точек в $X$ всегда равна единице, $P(\nu = 1) = 1$. Примем в качестве критерия пошаговой оптимизации величину $\gamma$, определяемую выражением:

$$\gamma = \max\{\Delta H\},$$

где $\Delta H$ - декремент неопределенности, определяемый количеством информации о состоянии объекта, получаемой, прямо или косвенно, в результате одного двоичного измерения.

Такой критерий называется аддитивным – декременты неопределенности шаг за шагом суммируются.

Задача оптимизации будет решена, если принять следующее разделение $X$ на подмножества перед первым шагом:

$$X_I^{\nu} = \{x_{\nu}\}, \quad P\{X_I^{\nu}\} = P(x_{\nu}) = 0{,}5;$$

$$X_{II}^{\nu} = \{x_{\nu+1}, x_{\nu+2}, \ldots, x_A\}, \quad P\{X_{II}^{\nu}\} = 0{,}5.$$

Таким образом, множество $X$ разделено на два равных по вероятности подмножества, что соответствует требованию оптимизации по критерию Шеннона-Фано.

Одновременно в процессе поиска осуществляется некоторое одно двоичное измерение.

Будем снабжать множества $X$ двумя индексами – верхним и нижним. Вверху указывается номер измерения $\nu$, совпадающий с номером шага поиска. При одном и том же $\nu$ могут осуществляться разные измерения $q$ (при разных путях движения по дереву поиска); они будут обозначаться внизу при $X$ в виде условных событий $q|\nu$.

Второй шаг оптимизации ($\nu = 2$) осуществляется в сцеплении с узлом $X_{II}^1$ на рис. 9 при следующих данных второй развилки (рис. 10).

Принимаются меры в порядке подготовки к $\nu = 2$ обеспечения равенства $P(X_{II}^2) = P(X_I^2)$ для получения максимально возможного количества информации от второго измерения ($\Delta H_2 = 1$ бит, $p = 0{,}5$).

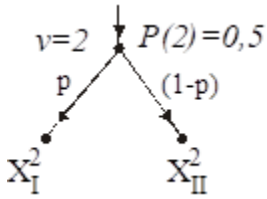


Рис. 10. Участок второй развилки

На рис. 11 развилки $\nu = 1$ и $\nu = 2$ приведены совместно. Перед нами два оптимизированных шага поиска в объединенном виде.

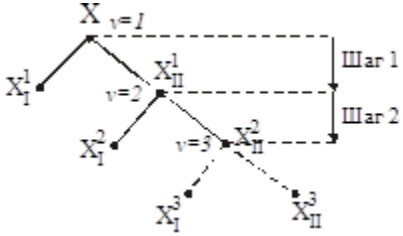

Рис. 11. Совместные развилки

В рассматриваемом случае распределения процедура легко наращивается. Применительно к подмножествам $X_I^2$ и $X_{II}^2$ их наполнение элементами множества $X$ приведено ниже:

$$X_I^2 = \{x_2\}, \quad P\{X_I^2\} = P(I|2) = p_2 = 0{,}5;$$

$$X_{II}^2 = \{x_3, x_4, ..., x_A\}, \quad P(X_{II}^2) = P(II|2) = 1 - p_2 = 0{,}5.$$

Индексы $\nu$ говорят о том, что речь идет о втором двоичном измерении.

*Равновероятное распределение.*

При равновероятном законе распределения вероятностей состояний исследуемого объекта вероятность любого из возможных состояний объекта определяется равенством:

$$P(x_i) = \frac{1}{A},$$

где $A$ - арсенал множества $X$.

Пусть $X$ симметричное множество. Это означает, по определению, что его арсенал $A$ поддается многократному делению на два без остатка.

Первый шаг оптимизации поисковой процедуры методом динамического программирования может быть представлен в виде рис. 12, а. При этом первый оптимизированный шаг поисковой процедуры получается путем деления $X$ на два равных (по сумме вероятностей элементов) подмножества $X_I^1$ и $X_{II}^1$. Вероятности $P(X_I^1)$ и $P(X_{II}^1)$ равны, и декремент неопределенности $\Delta H_1$ достигает максимально возможного значения в 1 бит. Вероятность первой развилки $P(1) = 1$,

вероятности подмножеств $X_I^1$ и $X_{II}^1$ равны каждая по 0,5 .

Второй оптимизированный шаг поисковой процедуры, получаемый путем деления каждого из предшествующих подмножеств $X_I^1$ и $X_{II}^1$ на 2, состоит из четырех параллельных путей (рис. 12, б) в направлении к финальным узлам при $A = 4$.

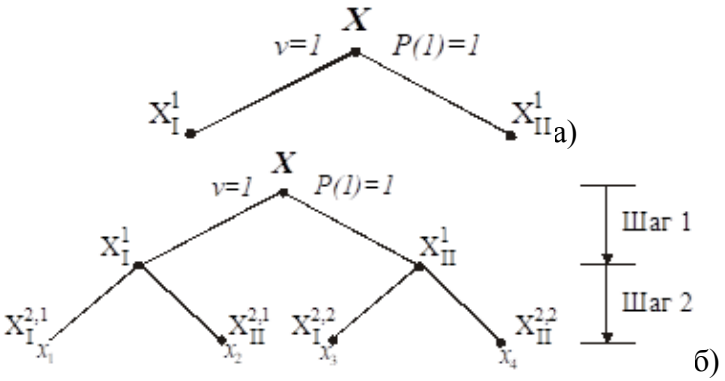


Рис. 12. Второй оптимизированный шаг

При $A = 8$ дерево поиска симметрично растет вниз до третьего шага поиска и заканчивается восемью финальными узлами соответственно.

На рис. 13 для иллюстрации приведено дерево поиска при равномерном распределении вероятностей состояний $P(x_i) = 1/5 = const$ и несимметричном множестве $X$ при $A = 5$. На рисунке просматриваются характерные черты как симметричного, так и несимметричного множеств.

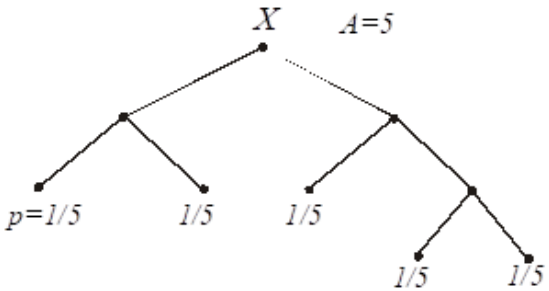


Рис. 13. Полное дерево поиска

*Лабораторное задание*

1. Включить режим дихотомического поиска. Установить число событий $A = 8$ для четного и $A = 16$ для нечетного варианта при равномерном распределении вероятностей и задать число измерений $n = 15$. Разработать оптимальный алгоритм поиска, задать его на наборном поле, провести моделирование, определить потенциальную скрытность.

2. Выбрать экспоненциальное распределение вероятностей событий вида $P_j = B \cdot 2^{-j}$, где $j = 1 \ldots A$, $B$ - нормирующий множитель, при том же $A$, что и в п. 1. Определить оптимальный алгоритм поиска и построить дерево поиска, задать его на наборном поле, провести моделирование, определить потенциальную скрытность.

Провести сравнительный анализ результатов п.1 и 2.

3. Для экспоненциального распределения вероятностей из п. 2 последовательно уменьшая максимальное число измерений от $n = 15$ до $n = \log_2 A$, разработать оптимальные алгоритмы поиска и по результатам моделирования определить соответствующие значения среднего числа измерений $R_{cp}$. Результаты занести в табл. 5.

4. Построить график зависимости $R_{cp}(N)$. Провести анализ результатов. Вывод – как изменяется оптимальный алгоритм поиска при ограничении максимального числа измерений – внести в отчет.

Таблица 5

| $n$ | 3 | 4 | … | 15 |
|---|---|---|---|---|
| $R_{cp}$ | | | | |

5. Для заданного варианта (в соответствии с последней цифрой номера зачетной книжки) распределения вероятностей при числе событий $A = 12$ разработать оптимальный алгоритм поиска, построить дерево поиска, объяснить, чем обусловлена его форма?

6. На наборном поле задать оптимальный полный алгоритм поиска. Последовательно исключая последние измерения (до

$n = 1$), рассмотреть зависимость среднего числа измерений $R$, вероятности неполного решения $P$ и остаточной скрытности $S_{ост}$ от продолжительности поиска $n$. Результаты записать в табл. 6, построить графики.

Таблица 6

| $n$ | 1 | 2 | … | 14 | 15 |
|---|---|---|---|---|---|
| $R$ | | | | | |
| $P$ | | | | | |
| $S_{ост}$ | | | | | |

*Содержание отчета*

1. Название, цель работы.
2. Определенная потенциальная скрытность.
3. Данные измерений и результаты расчетов.
4. Графики зависимости $R_{ср}(N)$.
5. Краткие выводы по результатам работы.

*Вопросы для самопроверки*

1. Критерии пошаговой оптимизации.
2. Оптимизация при усеченном показательном законе распределения вероятностей состояний.
3. Оптимизация поисковых процедур с учетом стоимости двоичных измерений и действия помех.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Основы теории скрытности [Текст]: учеб. пособие / З.М. Каневский, В.П. Литвиненко, Г.В. Макаров, Д.А. Максимов. – Воронеж: ВГТУ, 2006. – 202 с.

2. Литвиненко, В.П. Энергетическая скрытность сигналов и защищенность радиолиний [Текст]: учеб. пособие / В.П. Литвиненко. – Воронеж: ГОУВПО «Воронежский государственный технический университет», 2009. – 166 с.

3. Литвиненко, В.П. Основы теории скрытности: Практикум [Текст]: учеб. пособие / В.П. Литвиненко. – Воронеж: ГОУВПО «Воронежский государственный технический университет», 2010. – 105 с.

4. Литвиненко, В.П. Моделирование случайных процессов [Текст]: учебное пособие / В.П. Литвиненко, О.В. Чернояров. – Воронеж: Воронежский государственный технический университет, 2017. – 174 с.

**ОГЛАВЛЕНИЕ**

## ПРИЛОЖЕНИЕ

Варианты распределения вероятностей

| № | Распределение вероятностей | Значения параметров |
|---|---|---|
| 1 | $P(x_i)=\dfrac{\exp(-\alpha\cdot i)}{\sum_{k=1}^{A}\exp(-\alpha\cdot k)},\ i=\overline{1,A}$ | $A=16$<br>$\alpha=0{,}1$ |
| 2 | $P(x_i)=\dfrac{A+1-i}{A(A+1)-\sum_{k=1}^{A}k},\ i=\overline{1,A}$ | $A=12$ |
| 3 | $P(x_i)=\dfrac{i}{\sum_{k=1}^{A}k},\ i=\overline{1,A}$ | $A=16$ |
| 4 | $P(x_i)=\dfrac{i^2}{\sum_{k=1}^{A}k^2},\ i=\overline{1,A}$ | $A=10$ |
| 5 | $P(x_i)=\dfrac{A^2+1-i^2}{A(A^2+1)-\sum_{k=1}^{A}k^2},\ i=\overline{1,A}$ | $A=12$ |
| 6 | $P(x_i)=\dfrac{(A-1)!}{i!(A-1-i)!}p^i(1-p)^{A-1-k},\ i=\overline{0,(A-1)}$ | $A=10$<br>$p=0{,}35$ |
| 7 | $P(x_i)=\dfrac{\exp(\alpha\cdot i)}{\sum_{k=1}^{A}\exp(\alpha\cdot k)},\ i=\overline{1,A}$ | $A=10$<br>$\alpha=0{,}1$ |
| 8 | $P_i=\dfrac{p^i}{\sum_{k=1}^{A}p^k},\ i=\overline{1,A}$ | $A=12$<br>$p=0{,}8$ |
| 9 | $P(x_i)=\dfrac{i^{1/2}}{\sum_{k=1}^{A}k^{1/2}},\ i=\overline{1,A}$ | $A=12$ |

| | | |
|---|---|---|
| 10 | $P_i = \dfrac{\binom{M+i-1}{i}(1-p)^i}{\sum_{k=0}^{A-1}\binom{M+k-1}{k}(1-p)^k},\ i=\overline{0,(A-1)}$ | $A=12$<br>$M=5$<br>$p=0{,}35$ |
| 11 | $P(x_i) = \dfrac{\exp\left(-\alpha\cdot i^2\right)}{\sum_{k=1}^{A}\exp\left(-\alpha\cdot k^2\right)},\ i=\overline{1,A}$ | $A=16$<br>$\alpha=0{,}02$ |
| 12 | $P(x_i) = \dfrac{\exp\left(\alpha\cdot i^2\right)}{\sum_{k=1}^{A}\exp\left(\alpha\cdot k^2\right)},\ i=\overline{1,A}$ | $A=12$<br>$\alpha=0{,}005$ |
| 13 | $P(x_i) = \dfrac{\binom{M}{i}\binom{N-M}{A-1-i}}{\binom{N}{A-1}},\ i=\overline{0,(A-1)}$ | $A=8$<br>$N=20$<br>$M=11$ |
| 14 | $P_i = \dfrac{b^i}{i!\cdot\sum_{k=1}^{A}\frac{b^k}{k!}},\ i=\overline{1,A}$ | $A=10$<br>$b=7$ |
| 15 | $P(x_i) = \dfrac{\exp\left(-\alpha\cdot(i-\beta)^2\right)}{\sum_{k=1}^{A}\exp\left(-\alpha\cdot(k-\beta)^2\right)},\ i=\overline{1,A}$ | $A=12$<br>$\alpha=0{,}02$<br>$\beta=5$ |
| 16 | $P_i = \dfrac{b^{-i}}{i!\cdot\sum_{k=1}^{A}\frac{b^{-k}}{k!}},\ i=\overline{1,A}$ | $A=12$<br>$b=0{,}2$ |
| 17 | $P(x_i) = \dfrac{i^{1/3}}{\sum_{k=1}^{A}k^{1/3}},\ i=\overline{1,A}$ | $A=16$ |
| 18 | $P(x_i) = \dfrac{i^{-\frac{1}{2}}}{\sum_{k=1}^{A}k^{-\frac{1}{2}}},\ i=\overline{1,A}$ | $A=10$ |

# ТЕХНИЧЕСКАЯ ДИАГНОСТИКА И СКРЫТНОСТЬ

## МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к лабораторным работам
для студентов направления 11.04.01 «Радиотехника»
(магистерская программа «Радиотехнические средства обработки и защиты информации в каналах связи»)

**Составитель**
**Краснов** Роман Петрович

Компьютерный набор Р. П. Краснова

Издается в авторской редакции

Подписано к изданию 20.06.2025.
Уч.-изд. л 1,8.

ФГБОУ ВО «Воронежский государственный технический университет»
394006 Воронеж, ул. 20-летия Октября, 84