Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ
Кафедра Информационные системы

УТВЕРЖДАЮ
Проректор по УМР
_____С. В. Коньшин
"____"_____2015 г.

ОСНОВЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Методические указания к лабораторнымработам
для специальности 5В070300 -Информационные системы

СОГЛАСОВАНО

Начальник УМО
_____М.А. Мустафин
“_____”_____2015г

Председатель ОУМК
_____Б.К. Курпенов
“_____”_____2015г

Редактор АУЭС
_____ Н.М. Голева
“_____”_____2015г

Специалист по стандартизации
_____Н.К. Молдабекова
“_____”_____2015г

Рассмотрено и одобрено на заседании кафедры ИС
протокол № 8
от 03.02.2015 г.
зав. кафедрой ИС
_____ Ш.И. Имангалиев

Составители:
_____ Ш.И. Имангалиев,
_____ Ж.Г. Аренбаева

Алматы 2015

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Кафедра информационных систем

ОСНОВЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Методические указания по выполнению лабораторных работ для специальности 5В070300 -Информационные системы

Алматы 2015

Составители: Ш.И. Имангалиев, Ж.Г. Аренбаева.

ОСНОВЫ ИНФОРМАЦИОННЫХ СИСТЕМ. Методические указания к лабораторным работам для специальности 5В070300 - Информационные системы. Алматы: АУЭС, 2015. - 36 с.

Настоящие методические указания составлены в соответствии с учебной программой курса «**ОСНОВЫ ИНФОРМАЦИОННЫХ СИСТЕМ**»для бакалавров специальности 5В070300 -Информационные системы.

Ил.14 (рисунков – 9, таблиц - 5), библиография – 13 наименований.

Рецензент: зав.каф. ИКТ к.т.н., доцент К.С. Чижимбаева

Печатается по плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи» на 2015 г.

© НАО «Алматинский университет энергетики и связи», 2015 г.

Сводный план 2013г. поз.190

Шнар Ихсанович Имангалиев,
Жанат Галимовна Аренбаева.

ОСНОВЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Методические указания по выполнению лабораторных работ
для специальности 5В070300 -Информационные системы

Редактор Н.М.Голева
Специалист по стандартизации Н.К. Молдабекова

Подписано в печать __.__.__.
Тираж 50 экз.
Объем ……. уч.-изд. л.

Формат 60x84 1/1

Бумага типографическая №1
Заказ _____ Цена тг.

Копировально-множительное бюро
некоммерческого акционерного общества
«Алматинский университет энергетики и связи»
050013 Алматы, Байтурсынова, 126

Содержание:

Введение …..... 4
1 Теоретический обзор 5
2 Лабораторная работа №1. Исследование конструкции и электрических параметров кабельных линий связи 9
3 Лабораторная работа №2. Кодирование (шифрование) информации..... 15
4 Лабораторная работа №3. Декодирование (дешифрование) информации 19
5 Лабораторная работа №4. Применение компьютерных систем для моделирования информационных процессов 25
Список литературы 34

Введение

Современные информационные системы предназначены оказывать помощь специалистам, руководителям, принимающим решения, в получении ими своевременной, достоверной, необходимой информации. Достигается это с помощью новейших информационных технологий, которые основываются на применении компьютеров, активном участии пользователей в информационном процессе, высоком уровне дружественного пользовательского интерфейса, широком использовании пакетов прикладных программ общего и специального назначения, возможности доступа к удаленным базам данных и программам благодаря сетям ЭВМ.

Постоянно расширяющиеся сферы применения персональных компьютеров, их массовое использование, привело к необходимости формирования наиболее эффективной вычислительной техники. В настоящее время на их основе создаются и успешно функционируют локальные и многоуровневые вычислительные сети, представляющие собой интегрированные компьютерные системы обработки данных. Интегрированные системы обработки данных проектируются как сложный информационно-технологический и программный комплекс, поддерживающий единый способ представления данных, единый способ взаимодействия пользователей с компонентами системы и обеспечивающий информационные и вычислительные потребности специалистов в их профессиональной работе. Особое значение в таких системах придается защите информации при ее передаче и обработке.

В лабораторном практикуме рассматриваются краткий теоретический обзор и содержание лабораторных работ, соответствующих учебной программе курса «Основы информационных систем».

1 Теоретический обзор

В настоящее время высокие технологии развиваются очень стремительно, что позволяет собирать, анализировать, систематизировать, перерабатывать и выводить колоссальные объемы информации. Немаловажную роль играет и защита информации, которая обеспечивает состояние защищённости информационной среды организации, её формирование, использование и развитие.

Информация является одним из ценнейших ресурсов развития общества. Учитывая особенности информации её можно классифицировать по следующим признакам:

1) По области образования:

- производственная;
- экономическая;
- социальная;
- политическая;

- исследовательская.

2) *По месту возникновения:*

- входящая информация, которая поступает извне и отражает процессы, происходящие в производственной, экономической, социальной сферах общества;
- исходящая информация, которая после обработки используется для принятия управленческих решений в различных органах управления: правительстве, ведомствах, предприятиях и организациях.

3) По техническим средствам:

- телевидение, радио, периодическая печать;
- средства связи -телефон, телеграф, факсимильная связь, электронная почта, скайп;
- компьютерные сети.

4) По степени стабильности:

- статическая, неизменяемая или редко меняющаяся;
- динамическая, изменяется регулярно и является функцией от времени.

5) *По характеру назначения:*

- структурированная, определяющая обязанности субъектов управления;
- отчетная, выдаваемая в соответствии с установленными сроками.

6) *По степени обработки:*

- первичная, полученная из первоисточника;
- промежуточная, полученная в процессе обработки;
- сводная, полученная в результате обработки и анализа материала.

Сбор и регистрация данных

Сбор информации – это процесс целенаправленного получения и анализа информации о предметной области, в роли которой может выступать тот или иной процесс, объект и т.д. Цель сбора –подготовка информации к дальнейшей обработке и использованию в информационном процессе.

Операции сбора и регистрации данных осуществляются с помощью различных средств. Различают следующие способы сбора и регистрации данных:

- механизированный;
- автоматизированный;
- автоматический.

Механизированный способ сбора и регистрации информации осуществляется непосредственно человеком с использованием простейших приборов (весы, счетчики, мерная тара, приборы учета времени и т.д.).

Автоматизированный способ сбора и регистрации информации предполагает использование универсальных систем сбора и регистрации,

обеспечивающих совмещение операций формирования первичных документов и получения машинных носителей.

Автоматический способ сбора и регистрации информации используется при обработке данных в режиме реального времени. При этом информация с датчиков, учитывающих ход производства (выпуск продукции, затраты сырья, время работы оборудования и т.д.), поступает непосредственно в ЭВМ.

Передача данных

Передача данных – это перемещение данных в виде двоичных сигналов средствами электросвязи, как правило, для последующей обработки средствами вычислительной техники.

Технические средства передачи данных включают:

- аппаратуру передачи данных, которая соединяет средства обработки и подготовки данных с телеграфными, телефонными и широкополосными каналами связи;
- устройства сопряжения ЭВМ с аппаратурой передачи данных, которые управляют обменом информации - мультиплексоры передачи данных.

Запись и передача информации по каналам связи в ЭВМ имеет следующие преимущества:

- упрощается процесс формирования и контроля информации;
- соблюдается принцип однократной регистрации информации в первичном документе и машинном носителе;
- обеспечивается высокая достоверность информации, поступающей в ЭВМ.

Дистанционная передача данных в виде электрических сигналов может быть непрерывной во времени и дискретной, т.е. носить прерывный характер. Наиболее широко используются телеграфные и телефонные каналы связи. Электрические сигналы, передаваемые по телеграфному каналу связи, являются дискретными, а по телефонному - непрерывными.

В зависимости от направлений, по которым пересылается информация, различают каналы связи:

- симплексный (передача идет только в одном направлении);
- полудуплексный (в каждый момент времени производится либо передача, либо прием информации);
- дуплексный (передача и прием информации осуществляются одновременно в двух встречных направлениях).

Каналы связи характеризуются скоростью передачи данных, достоверностью, надежностью передачи. Скорость передачи определяется количеством информации, передаваемой в единицу времени и измеряется в бодах (бод = бит/сек). На практике существует множество вариантов технологических процессов обработки данных, которые зависят от использования различных средств вычислительной и организационной техники на отдельных операциях техпроцесса. Организация технологического

процесса зависит от характера решаемых задач, круга пользователей, от используемых технических средств, от систем контроля данных и т.д.

Обработка данных

Информационные технологии обработки данных применяются в целях автоматизации неэффективных, постоянно повторяющихся операций управленческого труда. Внедрение информационных технологий и систем существенно повышает производительность труда, уменьшаетмногочисленные рутинные операции, приводит к оптимизации численности работников.

Технологический процесс обработки информации с использованием ЭВМ включает в себя следующие операции:

- прием, подготовка, проверка и комплектование документов;
- ввод данных в ЭВМ;
- обработка данных;
- получение результатов обработки и их оформление.

Подавляющее большинство данных необходимо сохранять для дальнейшего использования, для их хранения и последующего применения создаются базы данных.

Вывод данных

Заключительным этапом обработки данных является их вывод в том или ином формате: графическом, табличном, текстовом или в виде формул. Непосредственно сам вывод данных осуществляется через различные устройства: принтеры различных видов (матричные, струйные, лазерные), монитор(дисплей) - устройство визуального отображения текстовой и графической информации, графопостроитель (плоттер), для вывода акустической информации – колонки, наушники, встроенные динамики.

2 Лабораторная работа №1. Исследование конструкции и электрических параметров кабельных линий связи

Цель работы: изучение конструкции современных кабельных линий связи, их электрических параметров, измерении и оценки искажений импульсов при передаче данных по кабелям связи.

Основные теоретические положения

В локальных компьютерных сетях используются в настоящее время три основные группы кабелей: коаксиальный, симметричный кабель типа «витая пара» и оптоволоконный. В первых двух типах кабеля в качестве среды распространения сигнала используется медная жила, а в оптическом кабеле - световод (оптоволокно). Выбор сетевого кабеля для конкретной сети зависит от ряда факторов, в число которых входят простота установки, требования к уровню защиты, скорость передачи (в Мбит/с) и затухание сигнала, а также стоимость кабеля.

Существуют две технологии передачи данных: широкополосная и узкополосная. При широкополосной передаче с помощью аналоговых сигналов в одном кабеле одновременно организуется несколько каналов. При узкополосной передаче канал всего один, и по нему передаются цифровые сигналы.

Электрические характеристики кабелей связи

Электрические свойства проводных линий характеризуются их основными, или первичными параметрами, отнесенными к одному километру длины. Первичными параметрами цепи ЛС являются:

1) активное сопротивление R, [Ом/км];
2) индуктивность L, [Гн/км];
3) емкость между проводами C, [Ф/км];
4) проводимость изоляции между проводами G, [См /км].

Сопротивление проводов зависит от их диаметра и материала. На сопротивление проводов влияет температура окружающей среды. Индуктивность и емкость линии определяется, в основном, расстоянием между проводами и диаметром проводов. Емкость кабельных линий, кроме того, зависит также от материала диэлектрика между проводами.

Проводимость изоляции воздушных линий зависит от погоды, а кабельных - от типа изоляции. Линии связи, у которых первичные параметры остаются неизменными по всей длине, называются однородными. При расчетах однородных линий связи по первичным параметрам пользуются эквивалентной схемой для 1 км цепи (рисунок 2.4).

Сопротивление — устаревшее название резистора, пассивного элемента электрической цепи, в идеале характеризуемого только сопротивлением

электрическому току.

Сопротивление медной жилы определяется главным образом сечением, т.к. при повышении частоты наблюдается так называемый поверхностный эффект. При поверхностном эффекте вихревые токи от переменного магнитного поля проводника с током взаимодействуют с током этого же проводника. В центре проводника эти токи направлены встречно, а по краям попутно вызвавшему их току. В результате плотность тока увеличивается по мере удаления от центра проводника к его поверхности. Внутренние слои проводника при этом практически не используются.

Кроме этого, в соседних парах проводников кабеля проявляется эффект близости за счет взаимодействии вихревых токов, наведенных магнитным полем одного проводника в соседнем проводе с основным током в этом проводнике. В результате такого взаимодействия происходит перераспределение плотности тока во втором проводнике, при этом она увеличивается на взаимообращенных друг к другу сторонах проводников симметричной цепи в случае, когда токи в проводниках текут в противоположных направлениях и на взаимно удаленных поверхностях при одинаковом направлении токов.

Оба вышеназванных эффекта сказываются тем сильнее, чем выше частота протекаемого тока. Суммарное действие этих эффектов приводит к увеличению сопротивления жилы с ростом частоты. В случае многопроволочного проводника сопротивление дополнительно увеличивается за счет того, что вышеупомянутые эффекты наблюдаются в пределах каждой проволоки, и усиливаются тем, что радиус этих проволок мал. Поэтому площадь сечения проводника многопроволочных жил выбирается несколько большей по сравнению со сплошной жилой.

Электрическая ёмкость — характеристика проводника, показывающая способность проводника накапливать электрический заряд.

Емкость двухпроводной линии на единицу длины определяется как:

$$C = \frac{\varepsilon}{18 \ln\left(\frac{D}{d}\right)} 10^{-6} \Phi / км \quad ,$$

где s-коэффициент диэлектрической проницаемости изоляции, Di d-диаметры изоляции и медной жилы соответственно, мм. Как видим, если исключить незначительные изменения s от частоты, емкость на высоких частотах не меняется. Коэффициент диэлектрической проницаемости зависит от материала изоляции, например, у полиэтилена он равен 2,2-2,3, а у пенополиэтилена - 1,2-1,5, что существенно улучшает вторичные параметры.

Электрическая проводимость (электропроводность, проводимость) — способность тела проводить электрический ток, а также физическая величина, характеризующая эту способность и обратная электрическому сопротивлению.

Проводимость изоляции на единицу длины определяется выражением:

$$G = \omega C tg\delta,$$

где С - емкость единицы длины кабеля, Ф; ю - угловая частота, рад/с; 8 - угол диэлектрических потерь. Из формулы видно, что проводимость растет с увеличением частоты.

Индуктивность (или коэффициент самоиндукции) — коэффициент пропорциональности между электрическим током, текущим в каком-либо замкнутом контуре, и магнитным потоком, создаваемым этим током через поверхность, краем которой является этот контур.

Индуктивность двухпроводной линии:

$$L = \left[4 \ln \frac{2a - d}{d} + Q(x) \right] 10^{-4} \quad Гн / км,$$

где *a*- расстояние между проводниками, мм; *d*- диаметр проводника, мм; *Q(x)*- коэффициент учитывающий внутрипроводниковую индуктивность, который уменьшается с ростом частоты, вследствие поверхностного эффекта; х - параметр, который для медных проводов определяется следующим образом

$$x = 7{,}09\sqrt{f /(10^4 \cdot R_t)}.$$

Здесь *ƒ*-частота сигнала в Гц, R_t-сопротивление жил кабеля при температуре t^0C, Ом. Для *x* больше 10 Q(x)=2 $\sqrt{2}$ / *x*.

Переходные затухания - NEXTи FEXT. В кабелях на основе витой пары передача информации происходит по двухпроводным цепям, расположенным рядом под общей оболочкой. Электромагнитные поля соседних цепей оказывают воздействие друг на друга, что приводит к искажениям полезного сигнала и ухудшению качества связи, в частности, в сетях передачи данных - к "потерянным пакетам".

Количественно этот параметр оценивают при помощи переходного затухания. Переходное затухание подразделяется на 2 величины - переходные затухания на ближнем и на дальнем концах (В иностранной литературе: NEXT - *Near-End-Crosstalk* и FEXT - *Far-End-Crosstalk).*

Для вычисления NEXT используется отношение излученной мощности сигнала к мощности, пришедшей вследствие наведенных токов на тот же конец кабеля, на котором расположен генератор:

$$NEXT = 20/\lg(U_{10}/U_{20}),$$

где NEXT (или a_0) - переходное затухание на ближнем конце, дБ; U_{10} - напряжение на выходе генератора, В; U_{20} - напряжение, на ближнем от генератора концу подверженной влиянию линии, В.

$$FEXT = 10\lg(U_{10}/U_{21}),$$

где FEXT (или a_l) - переходное затухание на дальнем конце, дБ; U_{21} - напряжение на дальнем от генератора концу подверженной влиянию линии, В.

NEXT снижается с ростом линии, приходя к некоему стабильному значению. Это связано с тем, что влияющие токи уменьшаются по амплитуде по длине кабеля, и, следовательно, их вклад в общую картину наводок

становится все меньше и меньше и значение NEXT стабилизируется. Иная картина наблюдается с FEXT, где имеется явно выраженный минимум переходного затухания при определенной длине линии, а затем оно растет с длиной линии.

Защищенность - ACR. Под защищенностью (в иностранной литературе - ACR - *Attenuation/ CrosstalkRatio)* понимают разность между уровнем полезного сигнала и помехи в данной точке кабеля, или по определению:

$$ACR=10/lg(P_{1l}/ P_{2l})$$

Нетрудно убедиться, что ACR=NEXT-Attenuation, то есть ACRполностью зависит от других характеристик. Считается, что кабель (как, впрочем, разъем, шнур и весь тракт целиком) обеспечивает устойчивую полнодуплексную работу любого приложения с такой верхней граничной частотой, на которой параметр ACR составляет 10 дБ.

Искажения сигналов при передаче данных по кабелям связи

Различного рода помехи (шумы), амплитудно-частотные (АЧХ) и фазочастотные (ФЧХ) характеристики линий связи, изменение уровня и др. называют первичными характеристиками линий. Они позволяют выявить характер физических явлений, влияющих на достоверность приёма информации.

Под вторичными характеристиками линий связи понимают искажения краев посылок (единичных элементов) сигналов. Эти характеристики позволяют по результатам приёма прямоугольных посылок непосредственно судить о достоверности принимаемой информации.

Причинами искажений единичных элементов являются первичные характеристики КС (например, воздействие флуктационных и импульсных помех, неравномерность АЧХ ФЧХ).

Краевые искажения - это изменение длительности принятых единичных элементов по отношению к переданным. Удобнее пользоваться относительной величиной краевых искажений

$$\delta = \theta / \tau_0 \ * 100\% = (t_{max} - t_{min}) / \tau_0 * 100\% = B\,(t_{max}-t_{min}) *100\%.$$

Здесь B - скорость передачи сигналов, Бод; t_{max} и t_{mln} - соответственно максимальное и минимальное значения смещения характеристических моментов модуляции относительно характеристических моментов восстановления. Как видно из выражения, величина краевых искажений возрастает с увеличением скорости передачи сигналов.

Краевые искажения в свою очередь подразделяются на: преобладания $S_{пр}$, характеристические $\delta_{хар}$ и случайные $\delta_{сл}$. Если искажения отдельных посылок остаются постоянными во времени (по величине и знаку), то их относят к искажениям, называемыми преобладаниями.

Особенностью характеристических искажений является зависимость их величины от характера передаваемой последовательности. Длительность посылок на выходе при этом меняется в зависимости от вида предыдущих посылок.

Случайные искажения характеризуются тем, что в процессе передачи дискретной информации нерегулярно возникают искажения отдельных посылок или пачки посылок.

Случайные искажения вызываются обычно помехами и являются случайной величиной, меняющейся во времени. В общем случае принимаемые посылки подвержены действию искажений указанных типов одновременно

$$\delta_{общ} = \delta_{пр} + \delta_{хар} + \delta_{сл}$$

Описание лабораторной работы

Рисунок. 1 - Схема лабораторной установки

Структурная схема лабораторной установки изображена на рисунке 1. В ее состав входят: источник последовательности сигналов типа «точки», двухлучевой осциллограф; милливольтметр; сегменты кабелей связи (два сегмента витой пары и два сегмента коаксиального кабеля), а также терминатор коаксиального кабеля. На стенде имеется возможность соединения сегментов однотипных кабелей последовательно и подключение различных нагрузочных сопротивлений на выход кабеля.

Программа работы

4.1 Изучить конструкции коаксиального и симметричного кабелей связи

4.2 Определить параметры коаксиального кабеля.

4.3 Определить и представить в графической форме переходные затуханий для значений частоты сигнала 1.0, 2.0, 3.0, 5.0, 7.0, 10.0 МГц и построить зависимость переходных затуханий от частоты.

4.4 Определить параметры искажения сигналов при передаче данных по

кабелям связи.

Содержание отчета

5.1. Схема экспериментальной установки.

5.2. Таблицы и графики зависимостей переходного затухания сигнала от частоты.

5.3. Данные параметры искажения сигналов при передаче данных по кабелям связи.

5.4. Выводы по работе.

Контрольные вопросы

1. Дайте определение кабеля связи, нарисуйте его эквивалентную схему и охарактеризуйте основные параметры кабельной линии.

2. Приведите примеры различных кабелей связи для компьютерных сетей, называя их тип, категорию, параметры и область применения.

3. Чем отличается симметричный кабель от несимметричного и в каких единицах измеряется несимметричность?

4. В чем отличие подключения к сетевой карте компьютера толстого и тонкого кабеля?

5. В каких случаях для построения локальной сети используется толстый, а в каких тонкий кабель?

6. Что такое BNC-коннектор, расшифруйте и поясните его мнемонику и покажите на практике его использование.

7. От чего возникают переходные помехи и как их можно уменьшить?

8. Охарактеризуйте виды сигналов, передаваемых по кабельным линиям связи и обоснуйте требования к ним.

9. Как в Ethernet с шинной топологией обнаруживаются коллизии?

10. Как рассчитывается максимальная длина сегмента в тонкой Ethernet?

11. Зачем в сетевой карте сети Ethernet используется преобразователь постоянного напряжения 5 В в постоянное 9 В?

12. Почему сетевая карта сети Ethernet подключается к кабелю через трансформатор?

2 Лабораторная работа №2. Кодирование (шифрование) информации

Цель работы: знакомство с основами криптографии, освоение алгоритма кодирования «двойными перестановками», выполнение задания по данному алгоритму кодирования, описание технологии выполненной лабораторной работы.

Защита информации и криптография

Информационная безопасность организации – это состояние защищенности информационной среды организации, обеспечивающее её формирование, использование и развитие, то есть защита информации, функционирующей в организации, от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Защитой информации человек занимается с древних времен, применяя различные методы тайнописи или, говоря современным языком, криптографии.

Криптография (крипто и графия) – тайнопись, система изменения текста с целью сделать его непонятным для непосвященных лиц. Отцом криптографии считается великий архитектор Леон Батиста Альберти (1404-1472), который ввел многоалфавитные перестановки, а так же шифрирующие коды. Его книга, написанная в 1467 году, является первым содержательным трудом по криптографии.

В настоящее время шифрование – неотъемлемая часть современного мира, его используют не только специальные службы, но и обычные пользователи компьютера. Специалист в области вычислительной техники должен разбираться в многочисленных средствах шифрования, чтобы выбирать наиболее защищенные системы. В современных информационных технологиях крайне актуальной является защита информации от несанкционированного доступа. В качестве стандартной модели безопасности часто приводят следующую модель:

1) Конфиденциальность – доступ к информации осуществляют только субъекты, имеющие на это право.

2) Целостность – защита информации от несанкционированной модификации.

3) Подотчётность – обеспечение идентификации субъекта доступа к информации и регистрация его действий.

4) Достоверность – соответствие предусмотренным правилам, порядку, формам и результатам.

5) Подлинность –гарантия идентичности информации заявленным требованиям.

Целью несанкционированного проникновения в сеть предприятия может быть нанесение вреда: уничтожения данных, кража конфиденциальной информации и использование ее в незаконных целях, использование сетевой инфраструктуры для организации атак на фирмы компаньонов, кража средств со счетов и т.п.

Отдельная категория электронных методов воздействия − компьютерные вирусы и другие вредоносные программы. Они представляют собой реальную опасность для современного бизнеса, широко использующего компьютерные сети, интернет и электронную почту. Проникновение вирусов на узлы корпоративной сети может привести к нарушению их функционирования,

потерям рабочего времени, утрате данных, краже конфиденциальной информации и хищениям финансовых средств. Вирусная программа, проникшая в корпоративную сеть, может предоставить злоумышленникам контроль над деятельностью компании.

На информационную безопасность компании могут влиять разнообразные внешние факторы (угрозы): неправильное хранение, кража компьютеров и машинных носителей информации, форс-мажорные обстоятельства и т.д.

Таким образом, в современных условиях наличие развитой системы информационной безопасности становится одним из важнейших условий конкурентоспособности и даже жизнеспособности любой организации.

Главная причина проникновения в компьютерные сети – беспечность и неподготовленность пользователей. Это характерно не только для рядовых пользователей, но и для специалистов в области компьютерной безопасности. Вместе с тем, причина не только в халатности, но и в сравнительно небольшом опыте специалистов по безопасности в сфере информационных технологий. Связано это со стремительным развитием рынка сетевых технологий и самой сети Интернет.

На сегодняшний день существует большой арсенал методов обеспечения информационной безопасности:

1) средства идентификации и аутентификации пользователей;
2) средства шифрования информации;
3) средства контентной фильтрации;
4) инструменты проверки целостности содержимого дисков;
5) средства антивирусной защиты;
6) системы обнаружения уязвимости сетей.

Каждое из перечисленных средств может быть использовано как самостоятельно, так и в интеграции с другими. Это делает возможным создание систем информационной защиты для сетей любой сложности и конфигурации.

Данная лабораторная работа является первым знакомством с криптографией и посвящена простейшим шифрам кодирования информации.

Шифры перестановки

В простых шифрах, к которым относятся шифры перестановки, используются таблицы, которые дают простые шифрующие процедуры перестановки букв в сообщении. Ключом в них служат размер таблицы, фраза, задающая перестановку или специальная особенность таблиц. Перестановка без ключа — один из самых примитивных методов шифрования. Например, сообщение «НЕЯСНОЕ СТАНОВИТСЯ ЕЩЕ БОЛЕЕ НЕПОНЯТНЫМ» записывается в таблицу по столбцам. Пример для таблицы из 5 строк и 7 столбцов приведен на рисунок 2.

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Рисунок 2. Таблица шифрования методом «перестановка без ключа»

После того, как открытый текст записан колонками, для образования шифровки он считывается по строкам. Если его записывать группами по 5 букв, то получится: НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ. Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы. Объединение букв в группы не входит в ключ шифра и используется лишь для удобства записи не смыслового текста.

Более практический метод шифрования, называемый одиночной перестановкой по ключу, очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в виде ключа слово ЛУНАТИК, получим следующие таблицы (рисунок.3).

Л	*У*	*Н*	*А*	*Т*	*И*	*К*
4	*7*	*5*	*1*	*6*	*2*	*3*
Н	0	Н	С	Б	Н	Я
Е	Е	0	Я	0	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	0	Ы
Н	А	Т	Е	Е	Н	М

До перестановки

А	*И*	*К*	*Л*	*Н*	*Т*	*У*
1	*2*	*3*	*4*	*5*	*6*	*7*
С	Н	Я	Н	Н	Б	0
Я	Е	Т	Е	0	0	Е
Е	П	Н	Я	В	Л	С
Щ	0	Ы	С	И	Е	Т
Е	Н	М	Н	Т	Е	А

После перестановки

Рисунок 3. Таблицы шифрования

В верхней строке таблицы «до перестановки» записан ключ, а номера под ключом определены по естественному порядку соответствующих букв ключа в алфавите. Ключ – это любая (цифровая или символьная) последовательность, позволяющая беспрепятственно расшифровать полученное сообщение. Чаще всего ключ известен только принимающей и передающей сообщение стороне и хранится в секрете. С другой стороны, для криптоаналитика ключ - это цель его работы.

После шифрования получим следующий текст: СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА. Для дополнительного кодирования можно повторно зашифровать это сообщение. Такой способ известен под названием

двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длина строк и высота столбцов были иные, нежели в первой таблице. Кроме того, в первой таблице можно переставлять столбцы, а во второй - строки. Можно также заполнять таблицу различными способами. Такое заполнение таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более сложным.

Кроме одиночных перестановок используются еще двойные перестановки столбцов и строк таблицы с сообщением. При этом перестановки определяются отдельно для столбцов и отдельно для строк. В таблицу вписывается текст и переставляются столбцы, а потом - строки. При расшифровке порядок перестановок обратный, пример показан на рисунке 4:

	2	4	1	3
4	П	Р	И	Е
1	З	Ж	А	Ю
2		Ш	Е	С
3	Т	О	Г	О

Исходная таблица

	1	2	3	4
4	И	П	Е	Р
1	А	З	Ю	Ж
2	Е		С	Ш
3	Г	Т	О	О

Перестановка столбцов

	1	2	3	4
1	А	З	Ю	Ж
2	Е		С	Ш
3	Г	Т	О	О
4	И	П	Е	Р

Перестановка строк

Рисунок 4. Таблицы шифрования двойной перестановкой

Получается шифровка АЗЮЖЕ СШГТООИПЕР. Ключом к этому шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы. При приеме сообщения его необходимо дешифровать. Для этого используется ключ, который передается или по секретным каналам связи или при личной встрече. Ключ – столбцы 2413, строки 4123. Переставляя столбы и строки в порядке, записанном в ключе, получаем исходное сообщение «ПРИЕЗЖАЮ ШЕСТОГО».

Задание к лабораторной работе 2

1. Получить у преподавателя текст для кодирования.
2. Определить размеры таблицы (количество строк и столбцов), в которой будет размещен текст, подлежащий кодированию.
3. Выбрать ключевое слово для кодирования полученного задания;
4. Закодировать полученный текст (предложение, включающее не менее 16 символов) методом двойной перестановки.

Содержание отчета

1. Титульный лист.
2. Цель работы.
3. Краткий теоретический обзор.

4. Описание технологии выполнения лабораторной работы.
5. Результаты выполнения задания, выданного к лабораторной работе.
6. Выводы по лабораторной работе.

4 Лабораторная работа №3. Декодирование (дешифрование) информации

Цель работы: криптоанализ сообщений, зашифрованных алгоритмом двойной перестановки и декодирование сообщения.

Декодирование шифров перестановки

Криптоанализ – раздел криптологии, изучающий методы расшифровки (определения ключа или сообщения). Необходимо определить текст зашифрованного сообщения.

Был получен текст АЗЮЖЕ СШГТООИПЕР. Известно, что для шифрования был использован метод двойной перестановки в таблице 4х4. Криптоаналитику необходимо дешифровать закодированный текст. Сообщение АЗЮЖЕ СШГТООИПЕР укладывается в следующую таблицу (рисунок 5).

	1	2	3	4
1	А	З	Ю	Ж
2	Е		С	Ш
3	Г	Т	О	О
4	И	П	Е	Р

Рисунок 5. Исходная таблица для расшифровки сообщения

Метод расшифровки (декодирования) двойной перестановки основан на определении вероятности различных сочетаний букв и нахождении истинной последовательности столбцов в шифровальной таблице.

Для декодирования зашифрованного сообщения необходимо определить вероятности следования двух букв разных столбцов и выбрать наиболее вероятную последовательность. Вероятность следования одного столбца за другим $P_{столбца}$ равна произведению вероятностей двухбуквенных комбинаций во всех n строках этих двух столбцов:

$$P_{столбца} = P_{строки\ 1} \bullet P_{строки\ 2} \bullet \ldots \bullet P_{строки\ i} \bullet \ldots \bullet P_{строки n}.$$

Для упрощения счета используют следующую формулу:

$$\log P_{столбца} = \log P_{строки1} + \log P_{строки2} + \ldots + \log P_{строки n}.$$

Более того, как и в статических алгоритмах эффективного кодирования,

чаще используются не вероятности появления в текстах комбинаций из двух букв, не частоты встречаемости, а количество встретившихся двухбуквенных комбинаций в текстах.

Таким образом, для декодирования сообщений, зашифрованных методом двойной перестановки, принято использовать логарифмы числа встречающихся в текстах двухбуквенных комбинаций F(), которые приведены в таблице №1. Для исходной таблицы, приведенной на рисунке 4, получаем следующие результаты.

При следовании за первым столбцом второго, получим:
F(1→2) =F(АЗ) + F(Е) + F(ГТ) + F(ИП)=7+9+0+5=21.
При следовании за первым столбцом третьего получим:
F(1→3) =F(АЮ) + F(ЕС) + F(ГО) + F(ИЕ) =6+8+8+8=30.
При следовании за первым столбцом четвертого получим:
F(1→4) =F(АЖ) + F(ЕШ) + F(ГО) + F(ИР) =7+5+8+7=27.
Рассматривая все возможные варианты следования столбцов, получим:
F(2→1) = F(ЗА) + F(_Е) + F(ТГ) + F(ПИ) =8+7+1+7=23;
F(2→3) = F(ЗЮ) + F(_С) + F(ТО) + F(ПЕ) =0+9+9+8=26;
F(2→4) = F(ЗЖ) + F(_Ш) + F(ТО) + F(ПР) =1+5+9+9=24;
F(3→1) = F(ЮА) + F(СЕ) + F(ОГ) + F(ЕИ) =0+7+8+8=23;
F(3→2) = F(ЮЗ) + F(С_) + F(ОТ) + F(ЕП) =2+7+8+8=25;
F(3→4) = F(ЮЖ) + F(СШ) + F(ОО) + F(ЕР) =1+5+6+8=20;
F(4→1) = F(ЖА) + F(ШЕ) + F(ОГ) + F(РИ) =6+6+8+8=28;
F(4→2) = F(ЖЗ) + F(Ш_) + F(ОТ) + F(РП) =1+5+8+4=18;
F(4→3) = F(ЖЮ) + F(ШС) + F(ОО) + F(РЕ) =0+0+6+8=14.

Таблица 1 - Логарифмы числа встречающихся двухбуквенных комбинаций

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ь	Э	Ю	Я	
А	2	7	8	6	7	7	7	7	4	7	7	7	8	8	3	7	6	7	8	2	6	6	7	7	5	5	0	0	0	0	6	7	9
Б	7	1	1	0	1	6	2	2	6	0	5	6	3	5	7	2	7	5	0	7	0	5	4	1	0	5	5	7	2	2	0	3	5
В	8	0	5	0	4	8	0	3	7	1	6	7	5	6	8	4	6	6	6	6	0	3	0	1	3	0	0	8	2	0	0	4	8
Г	6	0	1	1	6	5	0	0	6	0	4	5	4	4	8	0	7	0	0	6	0	0	1	2	0	0	0	0	0	0	0	0	4
Д	8	1	6	3	4	8	1	0	7	0	4	7	1	7	8	4	6	5	2	7	1	3	3	3	4	0	0	6	4	0	4	5	7
Е	5	5	6	7	8	6	6	6	4	7	7	8	8	9	6	5	8	8	9	3	3	6	5	6	5	6	0	0	1	1	5	5	9
Ж	6	0	0	0	6	7	2	1	7	0	5	0	2	7	1	0	1	2	1	3	0	0	0	0	0	0	0	0	2	0	0	0	2
З	8	4	6	2	6	4	1	1	6	1	5	5	6	6	7	1	5	0	0	6	0	0	2	1	0	0	2	6	2	0	0	4	6
И	6	6	7	6	6	8	5	7	7	7	7	6	8	8	5	5	7	8	8	1	5	7	7	7	6	3	0	1	0	0	6	7	9
И	0	0	3	0	3	0	0	0	0	0	3	6	5	4	0	0	0	6	6	0	0	0	1	2	3	0	0	0	0	0	0	0	8
К	8	1	5	1	1	6	5	2	7	1	2	7	0	5	8	0	7	6	6	7	0	0	6	0	1	0	0	0	0	0	0	0	7
Л	8	4	1	2	1	8	6	1	8	0	4	4	1	6	7	0	0	3	3	6	3	0	0	3	1	1	0	6	8	0	7	8	6
М	7	5	7	2	2	8	0	1	7	0	4	4	7	6	8	5	1	3	1	6	1	0	0	0	0	0	0	7	3	0	0	6	8
Н	9	0	3	3	6	8	1	1	9	0	6	0	1	7	8	0	0	5	7	6	5	2	5	3	0	0	0	8	5	0	4	6	7
О	2	8	8	8	8	6	7	7	6	8	7	8	8	7	6	7	8	8	8	3	2	5	6	7	6	5	0	0	1	5	2	5	9
П	7	0	0	0	0	8	0	4	7	0	3	6	1	4	8	4	9	4	5	6	2	0	1	0	0	0	0	4	5	3	0	4	4
Р	9	1	6	4	4	8	6	0	8	0	5	2	6	6	8	4	2	6	6	7	3	5	4	2	4	2	0	7	4	0	1	6	7
С	6	4	6	2	5	7	2	0	7	0	7	8	6	6	8	7	5	6	9	6	3	5	1	5	5	0	0	5	6	1	3	8	7
Т	8	2	7	1	4	8	0	0	8	0	6	4	5	6	9	3	8	8	4	6	0	0	0	4	0	2	1	7	8	0	1	5	8
У	3	4	4	6	6	7	6	5	3	3	6	5	5	6	0	6	7	7	7	1	5	5	0	6	3	6	0	0	0	0	7	4	8
Ф	6	0	0	0	0	5	0	0	6	0	0	2	2	0	6	0	4	0	3	5	4	0	0	0	0	0	0	1	0	0	0	0	2
Х	4	3	3	0	0	4	0	0	3	0	1	1	0	5	6	0	5	3	1	3	0	0	2	0	0	0	1	0	0	0	0	0	8
Ц	5	0	6	0	0	6	0	0	7	0	0	0	0	0	3	0	0	0	0	4	0	0	0	0	0	0	0	5	0	0	0	0	5
Ч	7	0	1	0	0	8	0	0	7	0	6	1	0	6	2	0	1	0	7	3	0	0	0	1	3	0	0	1	3	0	0	0	4
Ш	5	0	0	0	0	6	0	0	7	0	3	3	0	3	4	0	3	0	3	4	0	0	0	0	0	0	0	0	4	0	0	0	5
Щ	6	0	0	0	0	7	0	0	6	0	0	0	0	2	0	0	2	0	0	4	0	0	0	0	0	0	0	0	4	0	1	0	1
Ъ	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	2
Ы	1	4	7	3	5	7	1	5	1	7	5	5	6	2	1	5	5	5	6	0	0	7	0	5	4	1	0	1	0	0	0	1	8
Ь	0	1	0	0	0	3	0	7	1	0	6	0	4	7	1	0	0	6	4	0	0	0	0	1	6	1	0	0	0	0	6	2	8
Э	0	0	4	0	0	1	0	0	0	2	6	5	2	1	0	2	0	1	7	0	4	3	0	0	0	0	0	0	0	0	0	0	1
Ю	0	5	0	0	2	0	1	2	0	4	1	0	0	0	0	0	0	3	7	0	0	0	0	6	1	7	0	0	1	0	3	0	7
Я	0	1	5	2	5	6	2	5	0	2	2	3	6	5	0	1	4	4	7	0	0	4	4	3	0	4	0	0	0	0	6	4	9
	7	8	9	7	8	7	5	8	8	3	8	6	8	9	9	9	8	9	8	7	7	6	7	8	5	1	1	2	1	8	2	6	0

На рисунке 6 приведен граф логарифмов частот следования столбцов друг за другом.

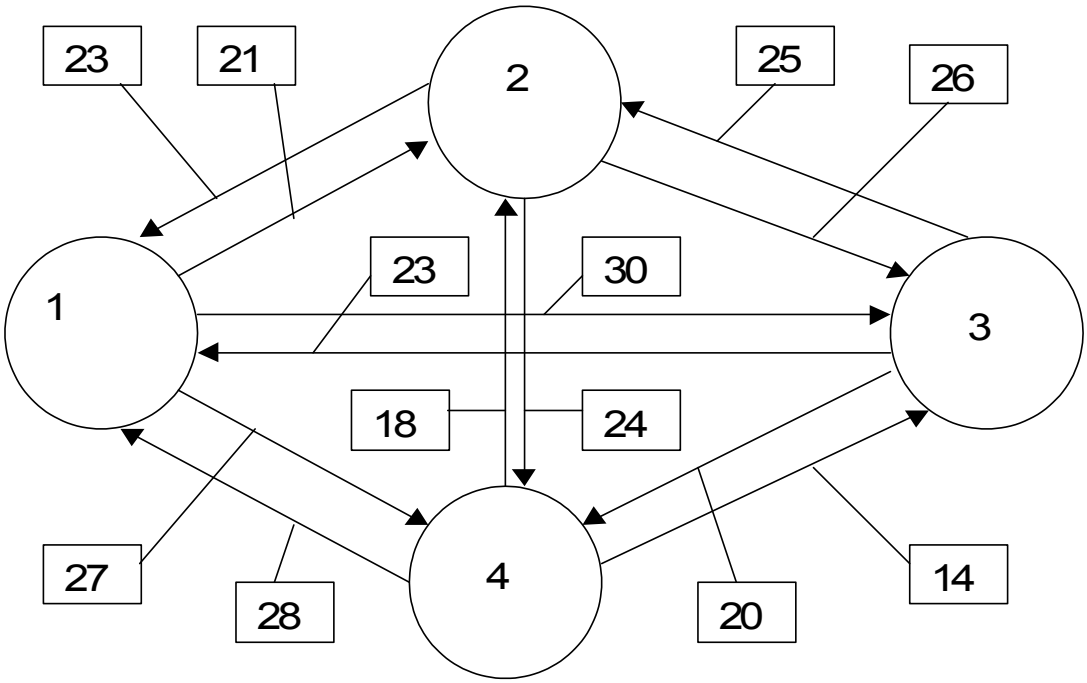


Рисунок 6. Граф логарифмов частот следования столбцов

Для дешифровки закодированного сообщения необходимо найти такой порядок следования столбцов, при котором получаем максимальную сумму логарифмов (наиболее вероятное следование столбцов в исходном сообщении). Существует множество методов решения этой задачи. Для простых случаев, как в данной лабораторной работе, целесообразно применить полный перебор вариантов. Результат решения приведен на рисунке 7.

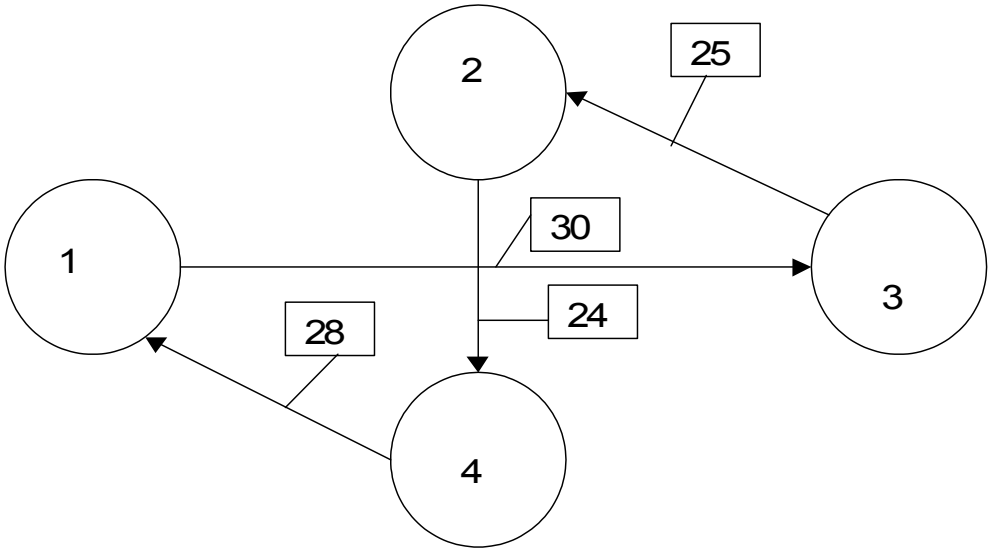


Рисунок 7. Подграф пути с максимальной суммой логарифмов

Составляем возможные варианты таблиц с учетом полученного графа (рисунок 8).

	1	3	2	4
1	А	Ю	З	Ж
2	Е	С		Ш
3	Г	О	Т	О
4	И	Е	П	Р

	4	1	3	2
1	Ж	А	Ю	З
2	Ш	Е	С	
3	О	Г	О	Т
4	Р	И	Е	П

	2	4	1	3
1	З	Ж	А	Ю
2		Ш	Е	С
3	Т	О	Г	О
4	П	Р	И	Е

	3	2	4	1
1	Ю	З	Ж	А
2	С		Ш	Е
3	О	Т	О	Г
4	Е	П	Р	И

Рисунок 8. Варианты таблиц, составленных на основе подграфа максимального пути

Текст в одной из них уже читается и, расставив строки в порядке (4123), получим расшифровку ПРИЕЗЖАЮ ШЕСТОГО (рисунок 9).

	2	4	1	3
4	П	Р	И	Е
1	З	Ж	А	Ю
2		Ш	Е	С
3	Т	О	Г	О

Рисунок 9. Расшифрованный текст

Задание к лабораторной работе 3

1) Произвести криптоанализ закодированного в лабораторной работе 1 сообщения.
2) сравнить полученный и исходные ключи.
3) разработать программы, позволяющие максимально автоматизировать процесс криптоанализа (автоматизированное рабочее место криптоаналитика).

Содержание отчета

1. Цель работы.
2. Краткий теоретический обзор.
3. Результаты выполнения задания, выданного к лабораторной работе.
4. Схемы алгоритмов для автоматизированного рабочего места криптоаналитика, листинги разработанных программ.
5. Выводы по лабораторной работе.

Контрольные вопросы:

1) Цель и задачи криптографии.
2) Шифры одиночной перестановки и перестановки по ключевому слову.
3) Шифры двойной перестановки. Шифрование с помощью магического квадрата.
4) Шифр многоалфавитной замены и алгоритм его реализации.
5) Алгоритм шифрации двойным квадратом.
6) Алгоритм шифрования RSA.
7) Алгоритм шифрования Эль Гамаля.
8) Задачи и алгоритмы электронной подписи.
9) Задачи распределения ключей.

5 Лабораторная работа №4. Применение компьютерных систем для моделирования информационных процессов

Цель работы: построение математической модели решения информационной задачи и нахождение оптимального результата решения,

обеспечивающего максимум доходов или минимум затрат в зависимости от условия задачи, применение приложения «Поиск решения» ППП MSExcel для нахождения оптимального решения.

Основные вопросы математического моделирования

С середины XX в. в самых различных областях человеческой деятельности стали широко применять математические методы и ЭВМ. Возникли такие новые дисциплины, как «Математическая экономика», «Математическая химия», «Математическая лингвистика» и т. д., изучающие математические модели соответствующих объектов и явлений, а также методы исследования этих моделей.

Математическая модель — это приближенное описание какого-либо класса явлений или объектов реального мира на языке математики. Основная цель моделирования - исследование объектов и событий, прогноз результатов будущих наблюдений с помощью математических методов, дающих возможность управлять объектами и явлениями, построение математических моделей изучаемых явлений.

Математическое моделирование состоит из следующих основных этапов:

1) Построение модели. На этом этапе выбирается некоторый объект - явление природы, конструкция, экономический план, производственный процесс и т. д. При этом, как правило, четкое описание ситуации затруднено. Сначала выявляются основные особенности явления и связи между ними на качественном уровне. Затем найденные качественные зависимости формулируются на языке математики, то есть разрабатывается математическая модель. Это самая трудная стадия моделирования.

2) Решение математической задачи с использованием разработанной модели. На этом этапе большое внимание уделяется разработке алгоритмов и численных методов решения задачи на ЭВМ, при помощи которых получен результат достаточной точности за оптимальное время.

3) Интерпретация полученных результатов. Решение, полученное на математическом «языке», интерпретируются в определениях и терминах решаемой задачи.

4) Проверка адекватности модели. На этом этапе выясняется соответствие результатов эксперимента с теоретическими следствиями из модели.

5) Модификация модели. На этом этапе происходит уточнение и корректировка модели, чтобы она была более адекватной действительности.

Для примера рассмотрим математическую модель задачи об определении надежности электрической цепи. Предположим, что в электрическую цепь последовательно включены три элемента, работающие независимо друг от друга. Вероятности отказов 1-го, 2-го и 3-го элементов соответственно равны следующим вероятностям: $P_1 = 0,1$, $P_2 = 0,15$, $P_3 = 0,2$.

Будем считать цепь надежной, если вероятность того, что в цепи не будет тока, не превышает 0,4 (P<= 0,4). Требуется определить, является ли данная цепь надежной.

Если откажет хотя бы один из элементов, то тока в цепи не будет, так как элементы включены последовательно. Пусть A_i — событие, заключающееся в том, что i-й элемент работает (i = 1, 2, 3). Тогда P(A1) = 0,9, P(A2) = 0,85, P(A3) = 0,8. Очевидно, что $A_1A_2A_3$ — событие, заключающееся в том, что одновременно работают все три элемента, и тогда:

$$P(A_1A_2A_3) = P(A_1)\bullet P(A_2)\bullet P(A_3) = 0{,}612.$$

В таком случае $P(A) + P(A_1A_2A_3) = 1$, отсюда $P(A) = 0{,}388 < 0{,}4$. Следовательно, цепь является надежной.

Приведенный пример отражает лишь одну из математических моделей и носит чисто демонстративный характер, далеко не исчерпывая всего многообразия математических моделей, возникающих в различных науках.

Задание к лабораторной работе

Мастер должен назначить на каждую из 10 операций по одному из имеющихся 12 рабочих. Время выполнения каждым рабочим одной из операций приведено в таблице. Знак вопроса в той или иной клетке таблицы означает, что данный рабочий не может выполнить эту операцию.

В рассмотренной задаче необходимо:

1) Разработать математическую модель задачи о назначениях с минимумом суммарных затрат времени на все операции;

2) решить задачу,используя приложение(надстройку) «Поиск решения» ППП MSExcel.

Таблица 2. Время выполнения операций

Рабочие	Операции									
	1	2	3	4	5	6	7	8	9	10
1	29	31	16	16	17	34	20	28	16	13
2	29	25	22	30	24	31	37	23	16	27
3	27	32	?	14	34	30	27	16	19	17
4	21	35	?	32	31	28	30	29	31	16
5	21	36	?	14	24	30	21	28	29	27
6	28	35	25	30	22	16	?	18	25	18
7	27	34	33	26	14	19	18	37	19	16
8	27	34	27	30	37	37	26	22	35	33
9	16	26	18	26	16	20	31	34	28	29
10	16	22	33	22	21	19	19	37	36	24
11	26	35	13	14	17	36	17	17	25	21

12	34	25	19	14	36	36	17	36	26	33

Построим математическую модель задачи:

$$c=\begin{pmatrix} 29&31&16&16&17&34&20&28&16&13\\ 29&25&22&30&24&31&37&23&16&27\\ 27&32&?&14&34&30&27&16&19&17\\ 21&35&?&32&31&28&30&29&31&16\\ 21&36&?&14&24&30&21&28&29&27\\ 28&35&25&30&22&16&?&18&25&18\\ 27&34&33&26&14&19&18&37&19&16\\ 27&34&27&30&37&37&26&22&35&33\\ 16&26&18&26&16&20&31&34&28&29\\ 16&22&33&22&21&19&19&37&36&24\\ 26&35&13&14&17&36&17&17&25&21\\ 34&25&19&14&36&36&17&36&26&33 \end{pmatrix}$$

Пусть x_i–работники, а x_j –операции (работы), тогда,

$x_{ij} = 1$, если i – работник выполняет j – работу (операцию),

$x_{ij} = 0$, если i – работник не выполняет j – работу (операцию),

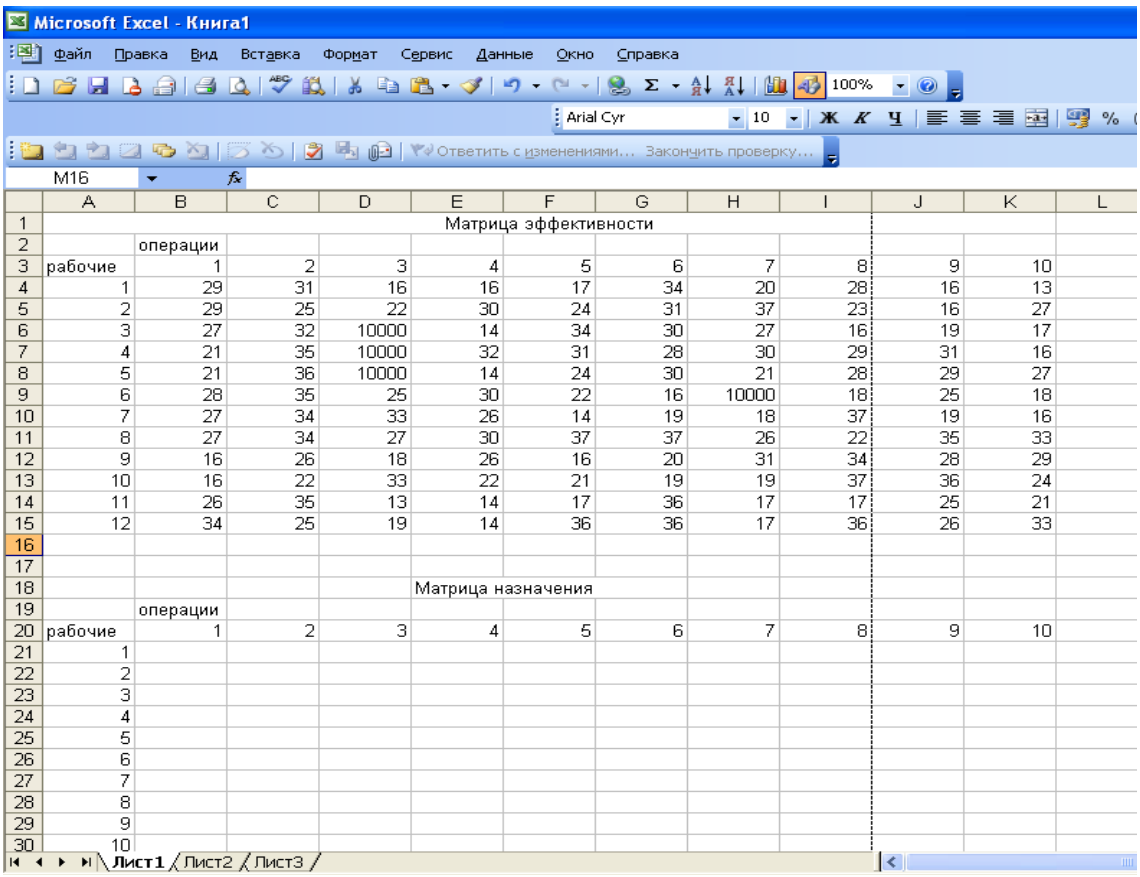
i изменяется от 1 до 12, jизменяется от 1 до 10.

Целевая функция имеет вид: $\sum_{j=1}^{10}\sum_{i=1}^{12} ¿\, c_{ij}\cdot x_{ij} \to min$

Ограничения:

$$\sum_{j=1}^{10} x_{ij} \leq 1 \qquad \sum_{i=1}^{12} x_{ij} = 1$$

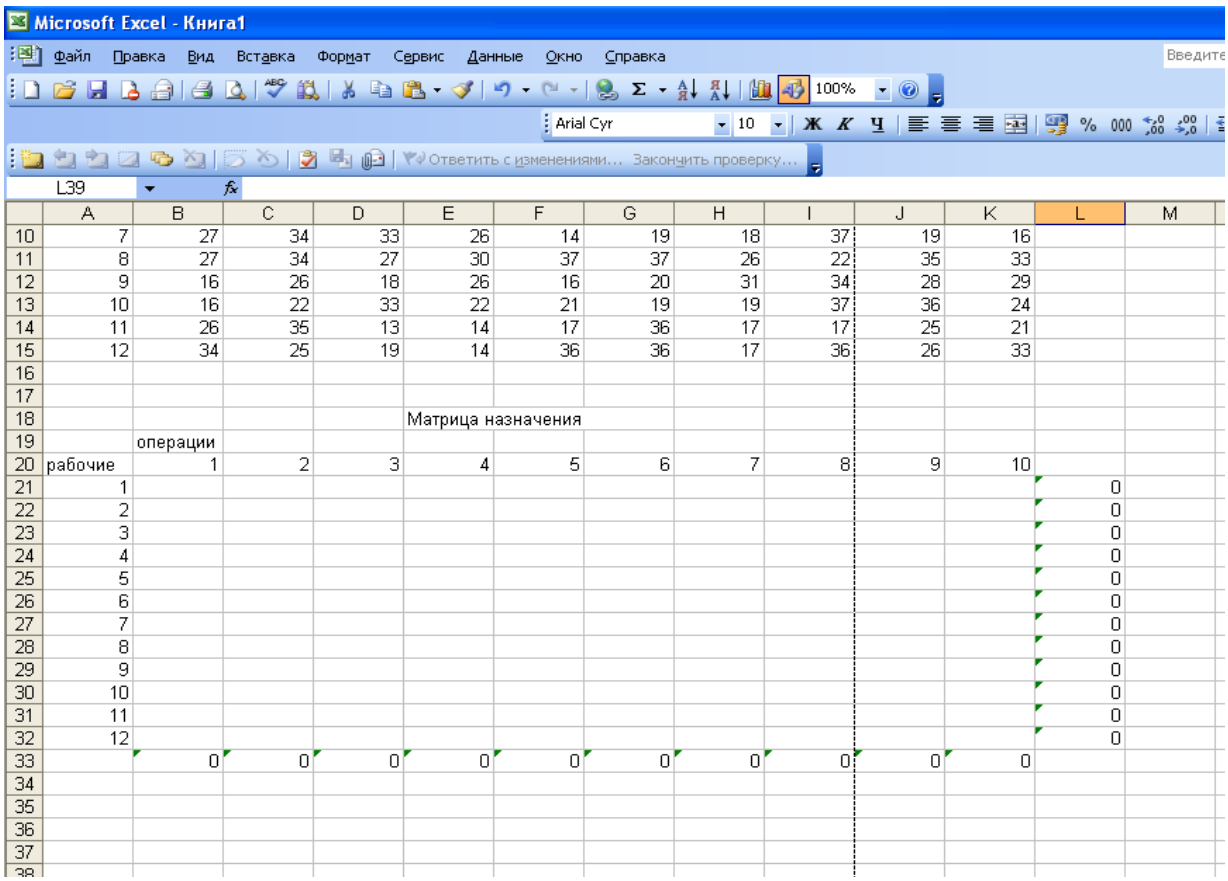
1.Построим две матрицы в MicrosoftExcel: матрицу назначения и матрицу времени.



	A	B	C	D	E	F	G	H	I	J	K	L
1	Матрица эффективности											
2		операции										
3	рабочие	1	2	3	4	5	6	7	8	9	10	
4	1	29	31	16	16	17	34	20	28	16	13	
5	2	29	25	22	30	24	31	37	23	16	27	
6	3	27	32	10000	14	34	30	27	16	19	17	
7	4	21	35	10000	32	31	28	30	29	31	16	
8	5	21	36	10000	14	24	30	21	28	29	27	
9	6	28	35	25	30	22	16	10000	18	25	18	
10	7	27	34	33	26	14	19	18	37	19	16	
11	8	27	34	27	30	37	37	26	22	35	33	
12	9	16	26	18	26	16	20	31	34	28	29	
13	10	16	22	33	22	21	19	19	37	36	24	
14	11	26	35	13	14	17	36	17	17	25	21	
15	12	34	25	19	14	36	36	17	36	26	33	
16												
17												
18					Матрица назначения							
19		операции										
20	рабочие	1	2	3	4	5	6	7	8	9	10	
21	1											
22	2											
23	3											
24	4											
25	5											
26	6											
27	7											
28	8											
29	9											
30	10											

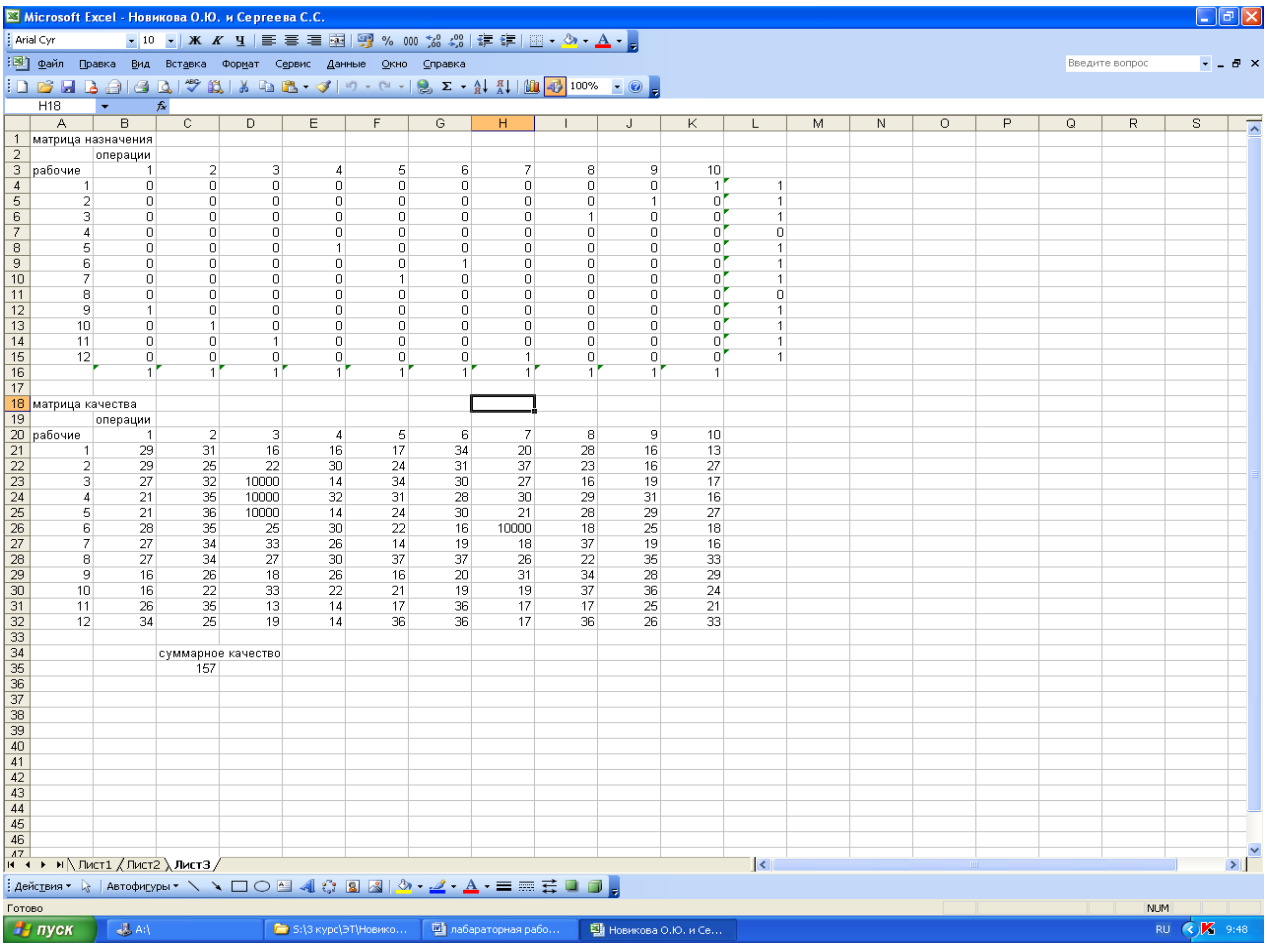
Лист1 Лист2 Лист3

В матрице назначения рассчитываем суммы по строкам и столбцам, для этого используем формулу СУММ.



	A	B	C	D	E	F	G	H	I	J	K	L	M
10	7	27	34	33	26	14	19	18	37	19	16		
11	8	27	34	27	30	37	37	26	22	35	33		
12	9	16	26	18	26	16	20	31	34	28	29		
13	10	16	22	33	22	21	19	19	37	36	24		
14	11	26	35	13	14	17	36	17	17	25	21		
15	12	34	25	19	14	36	36	17	36	26	33		
16													
17													
18					Матрица назначения								
19		операции											
20	рабочие	1	2	3	4	5	6	7	8	9	10		
21	1											0	
22	2											0	
23	3											0	
24	4											0	
25	5											0	
26	6											0	
27	7											0	
28	8											0	
29	9											0	
30	10											0	
31	11											0	
32	12											0	
33		0	0	0	0	0	0	0	0	0	0		
34													
35													
36													
37													

В целевую ячейку записываем целевую функцию, используя функцию СУММПРОИЗВ, где массив1 - ячейки матрицы времени, а массив 2 – изменяемые ячейки матрицы назначения. Затем, используя надстройку «Поиск решения», находим решение задачи. В параметрах указываем линейную модель, неотрицательные значения и распределение рабочих таким образом, чтобы время выполнения работ было минимальным:



Решение найдено: - 4 и 8 рабочие не назначены на какие–либо работы;

- остальные рабочие (1,2,3,5,6,7,9,10,11,12) назначены на определенный вид работ.

Для более глубокого исследования полученного решения можно проанализировать предлагаемые в приложении Поиск решения отчеты: отчет по результатам, отчет по устойчивости и отчет по пределам.

Отчет по результатам включает в себя 3 таблицы:

1) приводится исходное и окончательное значение целевой ячейки, в которую помещена целевая функция решаемой задачи;

2) приведены исходные и окончательные значения оптимизируемых переменных, которые содержатся в изменяемых ячейках;

3) содержится информация об ограничениях.

В таблице 2 графа Значение - показывает фактическое выполнения ограничении (левую часть), графа Разница показывает разность между необходимым количеством ресурсов и их наличием. Статус определяет, связанными или несвязанными являются те или другие ограничения (связанные – зависят, несвязанные – не зависят) с оптимальным решением. Если ресурс используется полностью, то в графе Статус указывается «связанное», при невыполнении ресурса в этой графе указывается «несвязанное».

Отчет по устойчивости состоит из двух таблиц. В этом отчете помещается информация об изменяемых переменных и ограничениях модели, что позволяет оценить, насколько чувствительным является полученное оптимальное решение к возможным изменениям параметров модели.

Нормированная стоимость показывает, насколько изменяется целевая функция при принудительном включении единицы этой продукции в оптимальное решение.

Теневая цена показывает выгодность ресурсов. Если теневая цена принимает нулевое значение, то изменение объема данного ресурса не приносит ни дохода, ни убытков. Если теневая цена принимает положительное или отрицательное значение, то изменение объема ресурса на одну единицу приносит соответствующий доход или убытки.

Отчет по пределам показывает, в каких пределах может изменяться выпуск продукции, вошедшей в оптимальное решение, при сохранении структуры оптимального решения.

Задание к лабораторной работе 4

1. Разработать математическую модель задачи.
2. Найти оптимальное решение задачи, используя приложение «Поиск решения» ППП MSExcel.
3. Кратко описать технологию работы с приложением «Поиск решения».
4. Привести краткие выводы по лабораторной работе.

Содержание отчета

1) Цель работы.
2) краткий теоретический обзор.
3) условие задания.
4) математическая модель решения задачи.
5) описание технологии работы с приложением «Поиск решения».
6) результаты выполнения варианта задания, выданного к лабораторной работе (скриншоты экранов).
7) выводы по лабораторной работе.

Контрольные вопросы:

1) Может ли целевая функция быть фиксированной?

2) Как формируются ограничения в задачах?

3) Что такое сценарий?

4) По какой команде выдается отчет сценария?

5) Как поступить, если программа выдала отрицательный результат?

Варианты заданий

1-й вариант

Фабрика изготовляет два вида красок: для внутренних и наружных работ. Для производства красок используются три исходных продукта A, B и C. Максимально возможные суточные запасы этих продуктов составляют 56, 80 и 117 т соответственно. Расходы продуктов A, B и C на 1 т соответствующих красок и максимально возможный запас приведены в таблице. Какое количество краски каждого вида должна производить фабрика, чтобы доход от реализации продукции был максимальным?

Таблица 3

Вид исходного продукта	Расход продуктов на 1 т красок		Суточные запасы исходных продуктов
	краска для наружных работ	краска для внутренних работ	
A	1	2	56
B	2	1	80
C	3	1	117
Оптовые цены 1 т красок	3	2	

2-й вариант

Компания занимается сборкой жидкокристаллических мониторов на заводе Квант. Поставки жидкокристаллических панелей и комплектующих деталей осуществляются из Кореи. Большую часть общей стоимости 15-дюймого ЖК-монитора составляет стоимость панели. Поэтому компания стремится минимизировать расходы на данный определяющий фактор.

В настоящее время основным поставщиком ЖК-панелей для компании является фирма CARDINAL. Однако фирма SYSCOM, давний партнер компании, вышла с новыми предложениями по поставке панелей в следующем году.

Таблица 4

CARDINAL		SYSCOM	
Количество	Цена, д.е.	Количество	Цена, д.е.
До 3000	204	До 5000	205

3000-6000	201	5000-10000	200
Свыше 6000	198	Свыше 10000	196

Издержки хранения панели оцениваются примерно в 31% в год от стоимости. Расходы по оформлению и доставке составляют 10000 ДЕ. Панели пакуются в стандартные короба по 96 штук. Планируемая потребность в будущем году - 50000 панелей. Определите, какой поставщик предлагает более выгодные условия. Какие панели и какой размер заказа следует выбрать при одинаковом качестве панелей и одинаковой стоимости доставки?

3-й вариант

Цех алкидных красок с производительностью 450 тонн продукта в месяц способен производить три разновидности красок: белой, синей и красной. Согласно договорам цех должен изготовить 40 тонн белой, 60 тонн синей и 80 тонн красной красок за месяц. Избыток краски сверх этого количества поступает в свободную продажу. В качестве сырья для изготовления красок используются четыре мастики в различных соотношениях. Цех располагает следующими запасами мастики: первой — 100 тонн, второй — 150 тонн, третьей — 120 тонн и четвертой — 180 тонн. Данные о расходе мастики на производство одной тонны каждой разновидности краски сведены в таблицу.

Таблица 5

Краски	**Расход мастики на 1 тонну краски, т**			
	Мастика 1	Мастика 2	Мастика 3	Мастика 4
Белая	0,3	0,2	0,4	0,4
Синяя	0,2	0,1	0,3	0,6
Красная	0,2	0,5	0,2	0,3

Требуется найти оптимальное (в смысле максимизации прибыли) количество каждого вида изготавливаемых красок при условии, что стоимости красок равны: белой – 13500 руб. синей — 11300 руб. и красной — 8200 руб. за тонну.

4-й вариант

Завод производит два вида электродвигателей Д1 и Д2 с производительностью 60 и 70 двигателей в день. Для Д1 требуется 10 единиц комплектующих изделий, а для Д2 — 8. Поставщик обеспечивает 800 единиц комплектующих. Доходность Д1 составляет 400 руб., а доходность Д2 — 300 руб. Максимизировать дневной доход при условии, что должно быть произведено не менее 10 единиц каждого электродвигателя.

-

Список литературы

1 Максимова О.В., Невзорова В.И. Информационные технологии для экономистов: Учебное пособие. – Ростов-на-Дону: Феникс, 2004.

2 Чернега В.С. Исследование конструкции и электрических параметров кабельных линий связи. – Севастополь: Изд-во СевНТУ, 2005.

3 Корнеев И.К., Ксандопуло Г.Н., Машурцев В.А, Информационные технологии: Учебник. – М.: Проспект, 2007.

4 Галатенко, В.А. Основы информационной безопасности. Интернет-университет информационных технологий. – М: INTUIT.RU, 2008.

5 Титоренко Г.А. Информационные системы в экономике. – М.: Юнити-Дана, 2009.

6 Щербаков, А.Ю. Современная компьютерная безопасность.
Теоретические основы. Практические аспекты. – М.: Книжный мир, 2009. – 352 с.

7 Грекул В.И. Проектирование информационных систем. – М.: Бином, 2010.

8 Блюмин А.М. Мировые информационные ресурсы– М.: Дашков и К, 2011.

9 Лебедько Е.Г. Теоретические основы передачи информации: Учебное пособие. – СПБ.: Лань, 201.

10 Шавенько Н.К. Основы теории информации и кодирования: Учебное пособие. – М,: Изд-во МИИГАиК, 2012. – 125 с.

11 Карпенков С.Х. Современные средства информационных технологии – М.: Кнорус, 2013.

12 Губарев В.В. Введение в теоретическую информатику: Учебное пособие. – Новосибирск: НГТУ, 2014.

13 Матвеев Б.В. Основы корректирующего кодирования: теория и лабораторный практикум: Учебное пособие. – СПБ.: Лань, 2014.