Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ
О ПРАКТИЧЕСКОЙ РАБОТЕ № 1
по дисциплине «Криптографические методы защиты информации»
ПОДСТАНОВОЧНЫЕ ШИФРЫ

Студент гр. БПИ196
Е.Н. Мосолков
«06» апреля 2021 г.

Руководитель
Заведующий кафедрой информационной безопасности киберфизических систем
канд. техн. наук, доцент
_____О.О. Евсютин
«___» _____ 2021 г.

Москва 2021

СОДЕРЖАНИЕ

1 Задание на практическую работу

Целью данной работы является приобретение навыков программной реализации и криптоанализа применительно к простым подстановочным шифрам.

В рамках практической работы необходимо выполнить следующее:

1. Написать программную реализацию шифров
    a. Шифр простой подстановки
    b. Аффинный шифр
    c. Аффинный рекуррентный шифр
2. Программная реализация должна обладать следующей функциональностью для всех реализованных шифров
    a. Принимать на вход произвольную последовательность символов, вводимую пользователем в качестве открытого текста или шифртекста;
    b. Принимать на вход секретный ключ вида, соответствующего конкретному шифру;
    c. Осуществлять зашифрование или расшифрование введенного текста по выбору пользователя.
3. Написать отчет, соответствующий требованиям
    a. Раздел с заданием;
    b. Раздел с краткой теоретической частью;
    c. Раздел с двумя-тремя примерами «ручного» шифрования для произвольных последовательностей символов;
    d. Раздел с результатами работы программы для тех же последовательностей символов, что и в предыдущем разделе;
    e. Раздел с примерами криптоанализа реализованных шифров;
    f. Раздел с выводами о проделанной работе.

2 Краткая теоретическая часть

2.1 Описание шифров

1. Шифр простой замены

Математически данный шифр может быть описан на языке подстановок. Каждой букве алфавита A мощностью m ставится в соответствие число из диапазона 1 ... m — другими словами, все символы алфавита нумеруются. Множество возможных ключей шифра простой замены является симметрической группой степени m, то есть группой подстановок длины m: $K = S(A) = Sm$. Открытый текст обозначим $x = (x1, ... , xl)$, где $xi \in A$, $i = 1, l$, соответствующий шифртекст — $y = (y1, ... , yl)$. Зашифрование открытого текста $x = (x1, ... , xl)$ на ключе $k \in K$ может быть записано как $Ek(x) = (k(x1), ... , k(xl))$, расшифрование шифртекста $y = (y1, ... , yl)$ на том же ключе — $Dk(y) = (k{-}1(y1), ... , k{-}1(yl))$, где $k{-}1 \in K$ — подстановка, обратная k. Проще говоря, при шифровании каждый символ текста заменяется на другой символ с помощью ключевой подстановки.

2. Афинный шифр

Данный шифр реализует замену символов открытого текста с использованием операций в кольце классов вычетов. Символы алфавита A мощностью m представляются элементами кольца классов вычетов Zm. В качестве ключа аффинного шифра выступает пара значений $k = (\alpha, \beta)$, $\alpha \in Zm*$, $\beta \in Zm$, соответственно ключевое пространство имеет вид $K = Zm * \times Zm$. Открытый текст и шифртекст обозначим соответственно $x = (x1, ... , xl)$ и $y = (y1, ... , yl)$, где $xi \in Zm$, $yi \in Zm$, $i = 1, l$. Зашифрование отдельного символа открытого текста осуществляется по формуле $yi = \alpha xi + \beta$, $i = 1, l$, расшифрование — по формуле $xi = (yi - \beta)\alpha - 1$, $i = 1, l$.

3. Афинный рекуррентный шифр

Данный шифр является усилением аффинного шифра, когда для каждого символа открытого текста вычисляется новое ключевое значение на основе предыдущего. Для этого необходимо задать две ключевые пары $k1 = (\alpha1, \beta1)$, $k2 = (\alpha2, \beta2)$, и тогда ключевая пара для произвольного символа преобразуемой последовательности будет иметь вид $ki = (\alpha i{-}1\alpha i{-}2, \beta i{-}1 + \beta i{-}2)$, $i = 3, l$.

2.2 Методы криптоанализа шифров

Частотный анализ – заключается в том, что если известен язык (источник) текста, то криптоаналитик сможет попытаться расшифровать текст, используя знания о характеристиках и признаках языка, например определить частоту появления каких-либо букв и сравнить их с частотой появления в текстах данного языка. Также закономерности наблюдаются на уровне присутствия конкретных слов, либо же перебираются частоты биграмм и триграмм слов из 2ух или 3х букв.

3 Примеры шифрования

Примеры «ручного» шифрования (зашифрование и расшифрование) с необходимыми пояснениями в части выбора параметров шифров.

Пример 1 – Шифр простой замены:

Строка для шифрования – “Hello world”

Возьмем произвольный ключ (алфавит) – “qazwsxedcrfvtgbyhnujmikolp”

Для зашифрования просто поставим под стандартным английским алфавитом наш ключ и переведем все символы сверху в символы снизу:

abcdefghijklmnopqrstuvwxyz

qazwsxedcrfvtgbyhnujmikolp

Берем первый символ H берем его строчное представление –

h переводим в символ e – получаем строку “E”

e переводим в символ s – получаем строку “Es”

l переводим в символ f – получаем строку “Esf”

повторяем для l – получаем строку “Esff”

o переводим в символ b – получаем строку “Esffb”

ставим знак разделения – получаем строку “Esffb ”

w переводим в символ k – получаем строку “Esffb k”

повторяем для o – получаем строку “Esffb kb”

r переводим в символ n – получаем строку “Esffb kbn”

повторяем для l – получаем строку “Esffb kbnf”

d переводим в символ w – получаем строку “Esffb kbnfw”

Получаем зашифрованный текст - “Esffb kbnfw”

Для расшифрования используем точно такой же алгоритм, только алфавит ставим вниз, а ключ – сверху.

Пример 2 – Афинный шифр:

Возмем строку “string” и зашифруем ее с помощью аффинного шифра, в качестве ключей возьмем пару чисел – 23, 30 – взаимно простые и максимально близкие к размеру алфавита числа. В качестве алфавита берем кодировку ASCII, тогда:

‘s’ = 115, (115 - 97 * 23 + 30) mod 26 + 97 = 99, ‘s’ переходит в ‘c’

‘t’ = 116, (116 - 97 * 23 + 30) mod 26 + 97 = 122, ‘t’ переходит в ‘z’

‘r’ = 114, (114 - 97 * 23 + 30) mod 26 + 97 = 102, ‘r’ переходит в ‘f’

‘i’ = 105, (105 - 97 * 23 + 30) mod 26 + 97 = 103, ‘i’ переходит в ‘g’

‘n’ = 110, (110 - 97 * 23 + 30) mod 26 + 97 = 114, ‘n’ переходит в ‘r’

‘g’ = 103, (103 - 97 * 23 + 30) mod 128 = 109, ‘g’ переходит в ‘m’

Получаем зашифрованую строку “czfgrm”

Для расшифровки строки “czfgrm” находим обратный элемент 23 по модулю 26 - это 17, далее расчитываем все символы по формуле (17 * (c – 97 - 30)) mod 26 + 97, где c – символ строки в ASCII

‘c’ = 99, (17 * (99 - 97 - 30)) mod 26 + 97 = 115, ‘c’ переходит в ‘s’

‘z’ = 122, (17 * (122 - 97 - 30)) mod 26 + 97 = 116, ‘z’ переходит в ‘t’

‘f’ = 102, (17 * (102 - 97 - 30)) mod 26 + 97 = 114, ‘f’ переходит в ‘r’

‘g’ = 103, (17 * (103 - 97 - 30)) mod 26 + 97 = 105, ‘g’ переходит в ‘i’

‘r’ = 114, (17 * (114 - 97 - 30)) mod 26 + 97 = 110, ‘r’ переходит в ‘n’

‘m’ = 109, (17 * (109 - 97 - 30)) mod 26 + 97 = 103, ‘m’ переходит в ‘g’

Получаем расшифрованую строку “string”

4 Программная реализация шифров

Особенности программной реализации и примеры работы программы.

Программная реализация сделана с использованием Jupiter notebook и языка python. При этом для корректного запуска и работы программы необходимо запустить все блоки кода по очереди. Разделение блоков на 4 части – “Substitution cipher”, “Affine cipher”, “Affine recurrent cipher” и “Program”.

Substitution cipher – представляет из себя 2 функции для шифровки и расшифровки простым подстановочным шифром с двумя примерами работы функций. Обе функции принимают в себя текст и алфавит длинны 26 (количество символов латинского алфавита в нижнем регистре), при этом для корректной работы функций необходимо передавать один и тот же алфавит, либо использовать алфавит по умолчанию

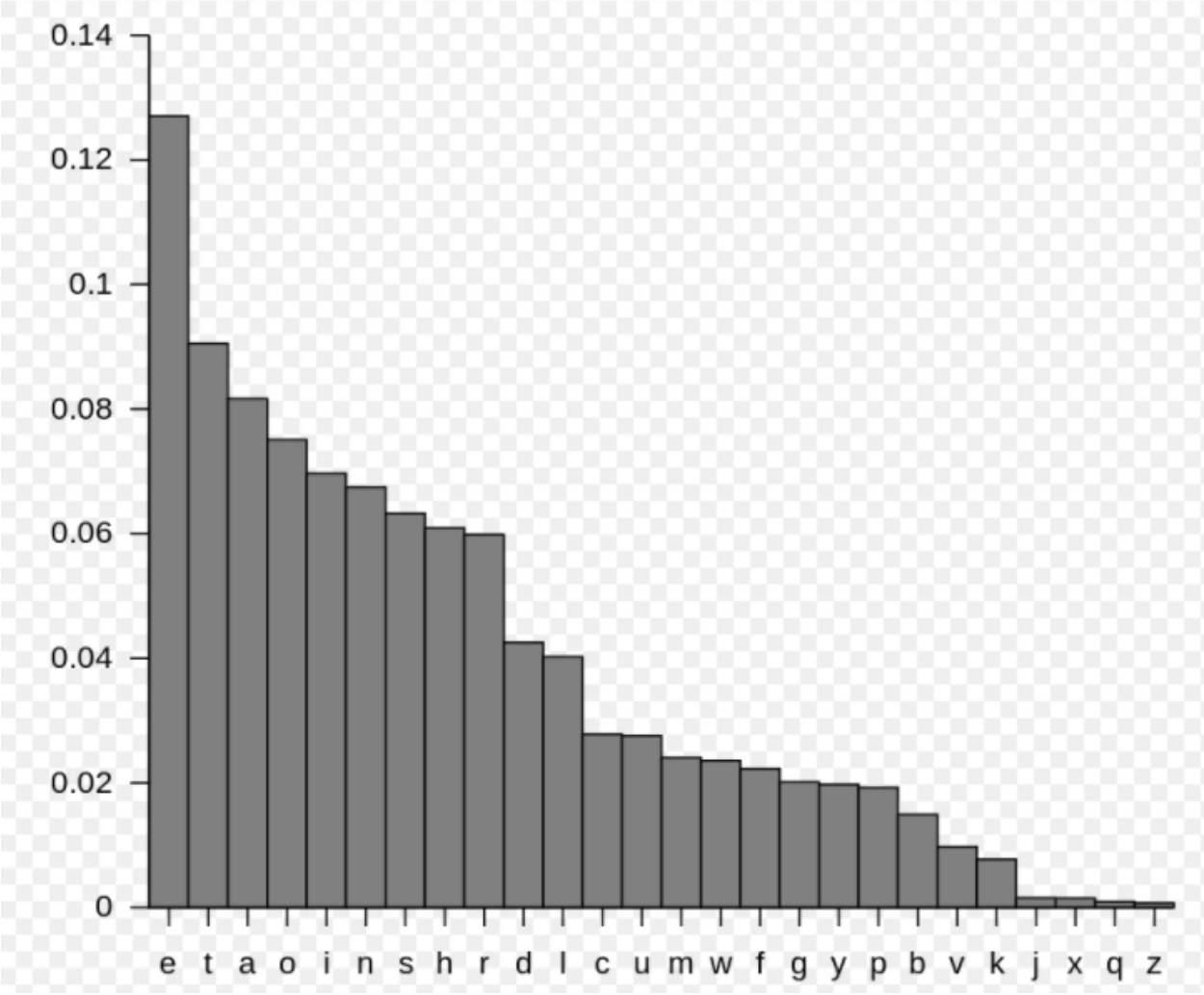
Affine cipher – представляет из себя 2 функции для шифрования и расшифрования аффинным шифром с двумя примерами работы функций. Обе функции принимают в себя строку и набор ключей – список из 2ух взаимно простых элементов ключей. Важно передавать для зашифрования и расшифрования один и тот же список ключей, либо использовать ключи по умолчанию.

Affine recurrent cipher - представляет из себя 2 функции для шифрования и расшифрования аффинным рекуррентным шифром, обе функции принимают в себя строку и два списка – 2 набора ключей для дальнейшей генерации пар ключей для шифрования или расшифрования символов строки.

5 Примеры криптоанализа

Частотный анализ строит предположение о том, что в достаточно больших текстах частоты одной и той же буквы равны, следовательно при моноалфавитном шифровании можно сравнить частоты появления символов в тексте и сделать выводы касательно букв, т.к. если частоты совпадают то скорее всего и буквы совпадают.

Частота встречи латинских букв в английских текстах



Рассмотрим зашифрованый текст - ‘A tpr opgi udk ndsaf wdv hphw’

Символы ‘d’, ‘p’ встречаются с частотой ‘13,04’

Символы ‘a’, ‘w’, ‘h’ встречаются с частотой ‘8,7’

Символы ‘t’, ‘r’, ‘o’, ‘g’, ‘i’, ‘u’, ‘k’, ‘n’, ‘s’, ‘f’, ‘v’ встречаются с частотой ‘4,35’

Скорее всего a => i || p => a, т.к. однобуквенное слово вероятно ‘I’ либо ‘A’

Предположим a => i и p => a, тогда получаем текст:

I _a_ _a__ ___ ___i_ ___ _a__

Теперь слово из трех букв скорее всего was, т.к. стоит после I

I was _a__ ___ ___i_ ___ _a__

Предположим, что o => d, либо e => d:

I was _a__ _o_ _o_i_ _o_ _a__, либо I was _a__ _e_ _e_i_ _e_ _a__

Пусть o => d, и 4e слово for, тогда

I was _a__ for _o_i_ _o_ _a__, логично предположить что следующее слово из 3х букв будет ‘you’

I was _a__ for _o_i_ you _a_y, далее буквы остаются только встречающиеся один раз. С таким коротким тестом трудно справиться частотным анализом, тем не менее используя немного брутфорса и знания рок призведений получаем строку из песни KISS ‘I was made for lovin you baby’

6 Выводы о проделанной работе

В рамках данной практической работы были изучены моноалфавитные шифры, такие как – шифр простой замены, аффинный шифр, рекурентный аффинный шифр, а также был произведен криптоанализ моноалфавитных шифров. Преимущество таких шифров – легкость шифрования – является их же недостатком, т.к. такой шифр можно взломать частотным анализом.

7 Список использованных источников

1. Шифр простой замены. – URL: https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B9_%D0%B7%D0%B0%D0%BC%D0%B5%D0%BD%D1%8B (дата обращения 11.04.2021)
2. Криптоанализ моноалфавитных шифров. – URL: https://morfey13.wikia.org/ru/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7_%D0%BC%D0%BE%D0%BD%D0%BE%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82%D0%BD%D1%8B%D1%85_%D0%B8_%D0%BF%D0%BE%D0%BB%D0%B8%D0%B0%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82%D0%BD%D1%8B%D1%85_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2. (дата обращения 11.04.2021)
3. Статистические методы криптоанализ. – URL: https://habr.com/ru/post/533974/ (дата обращения 11.04.2021)

ПРИЛОЖЕНИЕ А.

Основные требования к оформлению отчета

А.1 Общие требования к оформлению отчета

Шрифт: единый, рекомендуемый – Times New Roman,

Цвет: черный,

Размер: не менее 12 пт., одинаковый по всему отчету,

Выравнивание текста – по ширине,

Межстрочный интервал – полуторный (исключения: оформление титула, должностей в списке исполнителей, названий рисунков и таблиц),

Абзацный отступ – 1,25 см.,

Отступы и интервалы в тексте – 0 см.

Полужирный шрифт**:** применяют только для заголовков структурных элементов отчета, для заголовков разделов и подразделов основной части отчета.

Курсив: допускается для обозначения объектов и написания терминов. Курсив также может использоваться для *акцентирования внимания, выделения текста в отчете*, но при этом текст должен быть *того же кегля и гарнитуры*. Разрешается для написания определенных терминов, формул, теорем применять шрифты разной гарнитуры.

Размеры полей: левое – 3,0 см., правое – 1,5 см., верхнее и нижнее – 2,0 см.

Номера страниц – арабскими цифрами, *внизу по центру***.** Титульный лист включают в общую нумерацию страниц отчета. *Номер* страницы на титульном листе *не проставляют*. *Приложения* должны иметь общую с остальной частью отчета сквозную нумерацию страниц.

Оформление перечислений**:** перед каждым элементом перечисления следует ставить *тире* или, при необходимости ссылки в тексте отчета на один из элементов перечисления, вместо тире ставят *строчные буквы,* начиная с буквы "а" (за исключением – е, з, й, о, ч, ъ, ы, ь), после которой ставится скобка. Простые перечисления отделяются запятой, сложные – точкой с запятой.

НЕ допускается использование *данных знаков*:

- ➢
- ✓
- •

При наличии конкретного числа перечислений допускается использовать *арабские цифры* со скобками.

Перечисления приводятся с абзацного отступа – 1,25 пт., без отступов слева и выступов справа.

А.2 Оформление иллюстраций

К иллюстрациям относятся: чертежи, графики, схемы, диаграммы, фотоснимки.

Иллюстрации следует располагать в отчете *непосредственно после текста отчета*, где они упоминаются впервые, или на следующей странице (по возможности ближе к соответствующим частям текста отчета).

На все иллюстрации в отчете должны быть даны ссылки. При ссылке необходимо писать слово "рисунок" и его номер, например: "в соответствии с рисунком 2". *Не допускается* сокращение типа *Рис.5.*

Иллюстрации, за исключением иллюстраций, приведенных в приложениях, следует нумеровать арабскими цифрами сквозной нумерацией: Рисунок 1.

Допускается нумеровать иллюстрации в пределах раздела отчета. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой: Рисунок 1.1.

Если рисунок в отчете всего один, то он обозначатся: Рисунок 1.

Иллюстрации при необходимости могут иметь наименование и пояснительные данные (подрисуночный текст). Слово "Рисунок", его номер и через тире наименование помещают после пояснительных данных и располагают в центре под рисунком.

Пример оформления названия рисунка:

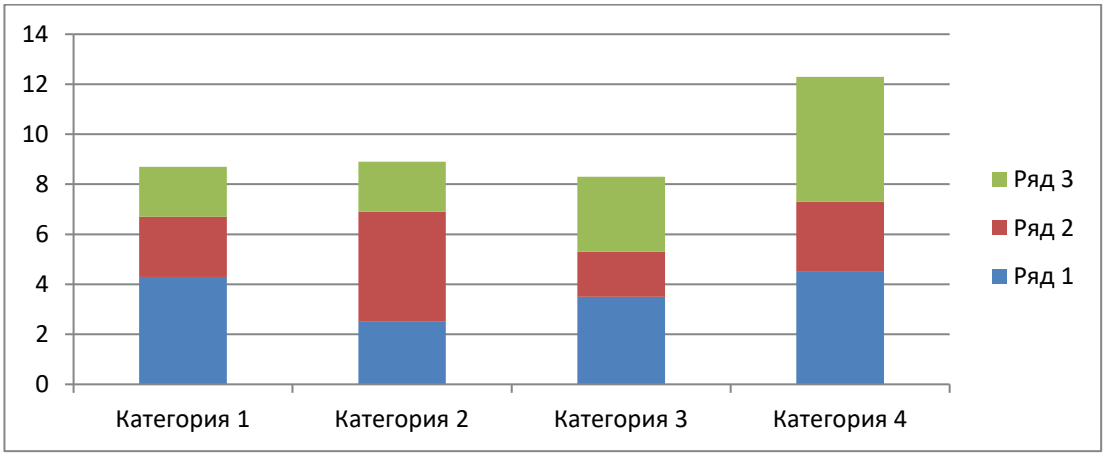


Рисунок 1.1 – Если наименование рисунка состоит из нескольких строк, то его записывают через один межстрочный интервал. Наименование рисунка приводят с прописной буквы без точки в конце. Перенос слов в наименовании рисунка не допускается

А.3 Оформление таблиц

Таблицу следует располагать непосредственно после текста, в котором она упоминается впервые, или на следующей странице.

На все таблицы в отчете должны быть ссылки. При ссылке следует печатать слово "таблица" с указанием ее номера**.** *Не допускается сокращение – Табл.*5.

Допускается применять размер шрифта в таблице меньший, чем в тексте отчета.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Допускается нумеровать таблицы в пределах раздела при большом объеме отчета. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенных точкой: Таблица 2.3.

Наименование таблицы следует помещать над таблицей слева без абзацного отступа в одну строку с ее номером через тире, например, Таблица 1 – Наименование. Наименование таблицы приводят с прописной буквы без точки в конце. Если наименование таблицы занимает две строки и более, то его следует записывать через *один межстрочный интервал*.

Если таблица занимает больше двух страниц, то при переносе части таблицы на другую страницу пишут слова «Продолжение таблицы 1», пример оформления названия таблицы:

Таблица 1.1 – Наименование таблицы следует помещать над таблицей слева без абзацного отступа с прописной буквы в одну строку с ее номером через тире без точки в конце. Если наименование таблицы занимает две строки и более, то его следует записывать через один межстрочный интервал

Продолжение таблицы 1.1

А.4 Оформление формул и уравнений

Уравнения и формулы следует выделять из текста в отдельную строку. Выше и ниже каждой формулы или уравнения должно быть оставлено *не менее одной свободной строки*. Если уравнение не умещается в одну строку, оно должно быть перенесено после знака равенства (=) или после знаков плюс (+), минус (–), умножения (×), деления (:) или других математических знаков. На новой строке знак повторяется.

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой они представлены в формуле. Значение каждого символа и числового коэффициента необходимо приводить с новой строки. Первую строку пояснения начинают со слова "где" без двоеточия с абзаца.

Формулы в отчете следует располагать *посередине строки* и обозначать порядковой нумерацией в пределах всего отчета арабскими цифрами в круглых скобках в крайнем правом положении на строке. Одну формулу обозначают (1).

Ссылки в отчете на порядковые номера формул приводятся в скобках в формуле (1).

Допускается нумерация формул в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой: (3.1)

Пример:

Для рядов данных *x, y* коэффициенты линейных зависимостей *a, b (y = a + bx)* рассчитываются, как решение системы уравнений (3.1):

$$\begin{pmatrix} 1 & \bar{x} \\ \bar{x} & \bar{x^2} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \bar{y} \\ \overline{xy} \end{pmatrix}, \qquad (3.1)$$

где *x* – средние или максимальные значения температуры процессоров;

y – температуры на выходе бака;

$\bar{x}$, $\bar{y}$ – среднее арифметическое значение элементов ряда.

А.5 Оформление списка использованных источников

Список должен содержать сведения об источниках, использованных при составлении отчета. Сведения об источниках приводятся в соответствии с требованиями ГОСТ 7.1, ГОСТ 7.80, ГОСТ 7.82 (пример приведен в Приложении Б).

Сведения об источниках следует располагать в порядке появления ссылок на источники в тексте отчета и нумеровать арабскими цифрами с точкой и печатать с абзацного отступа.

Список использованных источников должен включать библиографические записи на документы, использованные при составлении отчета, ссылки на которые оформляют арабскими цифрами в квадратных скобках [1], [3]–[10] в тексте отчета. На каждый источник в тексте отчета должна быть такая ссылка.

ПРИЛОЖЕНИЕ Б.

Пример списка использованных источников

1. DeRidder J.L. The immediate prospects for the application of ontologies in digital libraries// Knowledge Organization – 2007 . – Vol. 34, No. 4 . – P. 227 – 246 .

2. Прогноз научно-технологического развития Российской Федерации на период до 2030 года . – URL: http://government.ru/media/files/41d4b737638891da2184/pdf (дата обращения 15.11.2016).

3. U.S. National Library of Medicine. Fact sheet: UMLS Metathesaurus/National Institutes of Health, 2006 – 2013. – URL: http://www.nlm.nih.gov/pubs/factsheets/umlsmeta.html (дата обращения 2014-12-09).

4. U.S. National Library of Medicine. Fact sheet: Unfied Medical Language System/National Institutes of Health, 2006 – 2013. – URL: http://www.nlm.nih.gov/pubs/factsheets/umls.html (дата обращения 2009-12-09).

5. Антопольский А.Б., Белоозеров В.Н. Процедура формирования макротезауруса политематических информационных систем// Классификация и кодирование – 1976 . – N 1 (57). – С. 25 – 29 .

6. Белоозеров В.Н., Федосимов В.И. Место макротезауруса в лингвистическом обеспечении сети органов научно-технической информации// Проблемы информационных систем – 1986 . – N 1. – С. 6 – 10 .

7. Гуреев В.Н., Мазов Н.А. Использование библиометрии для оценки значимости журналов в научных библиотеках (обзор)// Научно-техническая информация. Сер. 1. – 2015 . – N 2. – С. 8 – 19 .

8. Земсков А.И., Шрайберг Я.Л. Электронные библиотеки: учебник для вузов. – М: Либерея, 2003 . – 351 с.

9. Костюк К.Н. Книга в новой медицинской среде. – М.: Директ-Медиа, 2015. – 430 с.

10. Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги [Электронный ресурс]. – URL: http://bookhamber.ru/stat_2006.htm (дата обращения 12.03.2009).

11. Web of Science. – URL: http://apps.webofknowledge.com (дата обращения 15.11.2016).

12. Леготин Е.Ю. Организация метаданных в хранилище данных// Научный поиск. Технические науки: Материалы 3-й науч. конф. аспирантов и докторантов/отв. за вып. С.Д. Ваулин; Юж.-Урал. гос. ун-т. Т. 2. – Челябинск: Издательский центр ЮУрГУ , 2011 – С.

128 – 132 .

13. Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги [Электронный ресурс]. – 2006. – URL: http://bookhamber.ru/stat_2006.htm (дата обращения 12.03.2009).

14. Приказ Минобразования РФ от 19 декабря 2013 г. N 1367 "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры". – URL: http://www. consultant.ru/document/cons_doc_LAW_159671 (дата обращения 04.08.2016).

15. ГОСТ 7.0.96-2016 Система стандартов по информации, библиотечному и издательскому делу. Электронные библиотеки. Основные виды. Структура. Технология формирования. – М: Стандартинформ, 2016 . – 16 с.