Министерство связи и массовых коммуникаций Российской Федерации

Государственное образовательное учреждение
высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

Самара

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Государственное образовательное учреждение высшего профессионального образования
«Поволжский государственный университет телекоммуникаций и информатики»

Кафедра МСИБ

Методические разработки к лабораторной работе

Исследование трафика локальной сети посредством сетевого анализатора Wireshark»

для студентов специальностей 210406, 210400, 210403

Составители:
к.т.н., доц. Киреева Н. В.
асс. Буранова М.А.

Редактор:
д.т.н., проф. Зайкин В.П.

Рецензент:
д.т.н., проф. Васин Н.Н.

Самара 2010

Лабораторная работа № 1
Программные средства анализа сетей с коммутацией пакетов. Анализатор пакетов Wireshark

Цель работы: анализ работы локальной сети с использованием программного пакета Wireshark.

Ход работы

1) Отчёт по лабораторной работе необходимо оформить в MS Word, поэтому перед началом работы следует создать на рабочем столе документ Word, куда и будут вставляться данные с пояснениями.

2) После запуска программы Wireshark необходимо произвести настройку захвата пакетов данных. Для этого командой Options… меню Capture вызывается специальное окно, где на панели Stop Capture… установкой соответствующего флага и значения задаётся длительность захвата (20+n) с, где n – последняя цифра зачётной книжки. Перед нажатием кнопки [Start] необходимо организовать копирование файла с сервера. Для этого открыть список компьютеров рабочей группы (Мой компьютер→Сетевое окружение→Отобразить компьютеры рабочей группы) и из указанного преподавателем места перетащить файл на рабочий стол. После окончания захвата копирование отменяется.

3) Определить IP-адрес данной рабочей станции (Пуск→Подключение→ Отобразить все подключения→Подключение по локальной сети→Свойства→ Протокол Интернета (TCP/IP)) и её имя в сети (Мой компьютер→Просмотр сведений о системе→Имя компьютера).

4) Открыть окно статистики по адресам (Statistics→Endpoints) и на вкладке Ethernet снять данные о количестве переданных (Tx Packets) и принятых (Rx Packets) пакетов по каждому адресу.

5) Далее задаётся фильтр пакетов для отображения всех пакетов, посланных с сервера. Для этого в поле Filter необходимо ввести ip.src==<ip-адрес отправителя>, где вместо <ip-адрес отправителя> вводится адрес

сервера, с которого производилось копирование. После чего нажать [Apply].

6) После применения фильтра открыть окно общей статистики (Statistics→Summary) и записать статистические данные для всех собранных (Captured) пакетов и для отображённых (Displayed) после применения фильтра.

7) Аналогично пункту 2 задать фильтр для пакетов, отправленных данной рабочей станцией.

8) Записать статистические данные для отображённых пакетов (смотри пункт 3).

9) Открыть окно для построения графиков (Statistics→ IO Graphs) и в поле Filter для 1 и 2 графика задать фильтры, которые задавались в пункте 2 и пункте 4. В результате должны получиться 2 графика:

а) график интенсивности трафика (пакетов/с) от сервера;

б) график интенсивности трафика (пакетов/с) от данной рабочей станции.

Путём задания отсчётного интервала (Tick interval) и количества пикселей на отсчёт (Pixels per tick) установить такой масштаб, чтобы графики занимали всю длину окна. Скопировать графики нажатием на клавишу Print Screen и вставить их в отчёт. Установить единицы измерения по оси Y Bytes/Tick и снова скопировать графики. Сделать выводы по графикам.

10) Отчёт сохранить в папке на сервере.

Отчёт по лабораторной работе

1) схему сети с указанными на ней IP-адресами и именами;

2) распределение кадров Ethernet по MAC-адресам;

3) числовые характеристики собранного трафика отдельно для канала от сервера и от рабочей станции;

4) графики интенсивности трафика, переданного от сервера и от рабочей станции;

5) выводы из собранных материалов, обратить внимание на количество широковещательных пакетов.

Контрольные вопросы

1) Какие существуют средства анализа сети?

2) Что такое WinPCAP? Для чего предназначен WinPCAP?

3) Для чего предназначен программный пакет Wireshark? Какие существуют другие средства для сбора пакетов?

4) Дайте характеристику сети Fast Ethernet.

5) Формат MAC-адреса.

6) Форма записи и состав IP-адреса.

7) Виды IP-адресов.

8) Что такое интенсивность? Дать определение интенсивности.

9) Почему различаются диаграммы интенсивности байт/с и пакеты/с?

10) Назовите отличие коммутируемых сетей от сетей с разделяемой средой.

Лабораторная работа №2

Определение среднего коэффициента загрузки дуплексного канала передачи на реальной сети Fast Ethernet с помощью пакетного анализатора

Цель работы: определить коэффициент загрузки локальной сети при передаче данных от выделенного севера сразу нескольким рабочим станциям.

Описание схемы измерений

В данной работе необходимо организовать одновременную передачу данных с сервера файлов (S) (рисунок 3.1) на рабочие станции (WS). Для этого нужно сразу на нескольких рабочих станциях запустить процесс копирования ресурса (сетевой папки), размещённого на сервере. Ресурс должен быть достаточного размера. Достаточного – означает, что его размер будет достаточным, для того чтобы провести замеры трафика до окончания передачи данных.

При копировании канал от сервера к коммутатору загружен на 100%. Эта нагрузка на выходе коммутатора распределяется по рабочим станциям. Если рабочая станция будет осуществлять и копирование ресурса и сбор всех пакетов, передаваемых от сервера, неизбежно будут происходить потери пакетов, так как пропускная способность канала не может быть больше 100%. Для уменьшения потерь пакетов и увеличения точности измерений в данной работе используется зеркалирование трафика (SPAN). Данная функция осуществляет копирование всех данных, проходящих через определённый порт коммутатора на «зеркальный» порт. К «зеркальному» порту подключается станция, которая осуществляет захват пакетов [3].

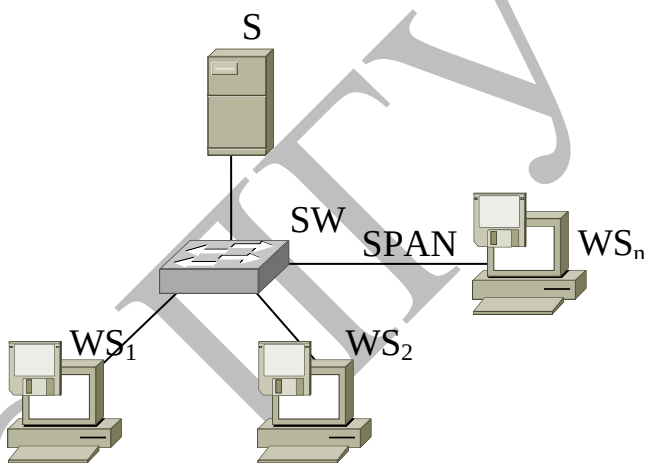


Рисунок 4.1 - Схема сети

Расчёт коэффициента загрузки канала

Коэффициент загрузки канала рассчитывается по формуле:

$$\rho = \frac{\sum \tau_i}{\sum v_i},$$

где τ_i – время обслуживания i-го кадра;

v_i – время от конца обслуживания i – 1 кадра до конца обслуживания i-го кадра.

Известно количество кадров и их размер (в байтах) и время измерения трафика. Тогда, не учитывая задержки среды, суммарное время обслуживания

$$\sum \tau_i = \frac{(L + N \cdot 24) \cdot 8}{B},$$

где

L – количество переданных (принятых) байт;

N – количество переданных (принятых) пакетов;

$N \cdot 24$ – не учтённые Wireshark межкадровый интервал, начальный ограничитель и преамбула;

B – скорость передачи в сети Fast Ethernet (100 Мбит/с).

$$\sum v_i = T,$$

где

T – время измерения трафика.

Тогда

$$\rho = \frac{(L + N \cdot 24) \cdot 8}{BT}.$$

Ход работы

1. На рабочей станции, которая будет осуществлять захват запустить программу Wireshark и подготовить её к сбору трафика (Capture→Options…→ выбрать интерфейс и длительность захвата 10 сек.).
2. Попросить преподавателя настроить коммутатор на зеркалирование трафика.
3. На двух других рабочих станциях запустить процесс копирования ресурса, указанного преподавателем.
4. После того, как одновременно обе станции начнут получать данные, запустить захват.
5. После окончания захвата копирование отменить.
6. Необходимо выделить одно направление дуплексного канала. Для этого необходимо задать фильтр ip.src == <IP-адрес отправителя> – для трафика с IP-адресом источника, ip.dst == <IP-адрес получателя> – для трафика с IP-адресом назначения.
7. Получить исходные данные для расчёта (Statistics→ Summary):
8. N – Packets – Displayed – количество захваченных пакетов, удовлетво-

ряющих условию фильтра;

9. L – Bytes – Displayed – общая длина всех пакетов, удовлетворяющих условию фильтра;

10. T – Between first and last packet – Displayed – время между первым и последним пакетом, удовлетворяющих условию фильтра.

11. Произвести расчёт. Сравнить со средней скоростью передачи Avg. Mbit/sec (Statistics→ Summary).

12. Сделать вывод о загрузке канала.

Отчёт по лабораторной работе

Отчёт по лабораторной работе включает:

1) схему измерения трафика с указанными на ней IP-адресами;
2) расчёт коэффициента загрузки канала;
3) выводы по полученным данным.

Контрольные вопросы

1) Формат кадра Ethernet.
2) Что показывает коэффициент загрузки канала?
3) Что представляет собой одноранговая сеть?
4) Что представляет собой сеть с выделенным сервером?
5) Как можно повысить эффективность работы сети с выделенным сервером?
6) Дайте сравнительную характеристику одноранговой сети и сети с выделенным сервером.
7) Назовите особенности схемы измерений данной лабораторной работы. Что такое зеркалирование трафика?
8) Что такое коммутатор? Каково его назначение?

Лабораторная работа №3

Определение статистических характеристик сетевого трафика

Цель работы: определить статистические характеристики сетевого трафика, характер распределения времени прихода пакетов и их размера при передаче данных различного типа.

Ключ к проектированию высокопроизводительных сетей заключается в способности моделировать и оценивать параметры производительности. Разработчик должен быть способен на основании наблюдений оценить объём и характеристики будущего трафика. Статистические характеристики трафика влияют на разнообразные аспекты проектирования и конфигурирования, включая протоколы маршрутизации, протоколы резервирования ресурсов, дисциплины очередей в маршрутизаторах и ATM-коммутаторах (Asynchronous Transfer Mode), а также размеры буферов. Более того, пользователь должен уметь охарактеризовать планируемый трафик, чтобы принять верные решения в области резервирования ресурсов.

Числовые характеристики случайной величины

Математическим ожиданием случайной величины называется сумма произведений всех возможных значений случайной величины на вероятности этих значений [4]. То есть,

$$M[X] = \sum_{i=1}^{n} x_i p_i ,$$

где x_i – i-ое значение случайной величины X;

p_i – вероятность x_i.

Математическое ожидание также называют средним значением случайной величины, так как оно показывает её местоположение на числовой оси и позволяет делать грубые расчёты.

При большом числе опытов n можно с достаточной точностью вычислить математическое ожидание как среднее арифметическое наблюденных значений случайной величины. В данной работе число опытов (пакетов в собранном дампе) позволяет делать такой расчёт, таким образом

$$M[X] = \frac{\sum_{i=1}^{n} x_i}{n}.$$

Дисперсией случайной величины X называется математическое ожидание квадрата отклонения этой случайной величины от её математического ожидания [4]. Или

$$D[X] = M[(X - m_x)^2],$$

где m_x – математическое ожидание X.

Дисперсия случайной величины есть характеристика рассеивания, разбросанности значений случайной величины около её математического ожидания.

Дисперсия случайной величины имеет размерность квадрата случайной величины; для наглядной характеристики рассеивания удобнее пользоваться величиной, размерность которой совпадает с размерностью случайной величины. Для этого из дисперсии извлекают квадратный корень.

Средним квадратическим отклонением случайной величины X называют квадратный корень из дисперсии:

$$\sigma[X] = \sqrt{D[X]}.$$

Модой случайное величины называется её наиболее вероятное значение [4]. Если кривая распределения имеет более одного максимума, распределение называется полимодальным.

Медианой случайной величины X называют такое значение *Me*, для которого одинаково вероятно окажется случайная величина меньше *Me* или больше *Me* [4].

Закон распределения случайной величины

Статистической функцией распределения случайной величины X называется частота события $X<x$ в данном статистическом материале [4], то есть:

$$F^*(x) = P^*(X < x).$$

Частота i-го события рассчитывается по формуле:

$$p_i = \frac{m_i}{N},$$

где m_i – число i-ых событий в выборке объёмом N.

Гистограмма распределения случайной величины – это график, по оси абсцисс которого откладывают возможные значения этой случайной величины, а по оси ординат соответствующие этим значениям частоты. При увеличении объёма выборки гистограмма распределения стремится к плотности вероятности этой случайной величины, которая показывает плотность, с которой распределяются значения случайной величины в данной точке.

Краткое описание используемых дампов

В качестве исходных данных для нахождения распределения и его числовых характеристик в данной работе используют уже собранные дампы трафика различных типов:

FTP – трафик передачи данных по сети Internet по протоколу File Transfer Protocol;

VoIP – трафик одной из наиболее популярных программ для IP-телефонии (Voice IP) – Skype;

WiFi (Wireless Fidelity) - трафик нового клиента сети WiFi (802.11) с авторизацией и активацией;

HTTP – захват трафика протокола гипертекстовых ссылок HiperText Transport Protocol содержащий немного jpeg-картинок;

Dial-Up – трафик HTTP при соединении по телефонному каналу (Dial-Up);

LAN (Local Area Network) – трафик передачи файла по локальной сети Fast Ethernet;

Counter Strike – трафик обмена данными между клиентом и сервером популярной on-line игры Counter Strike 1.6, подключение по технологии ассиметричной цифровой абоненской линии Asymmetric Digital Subscriber Line (ADSL);

FLV-Video (Flash Video) — трафик при просмотре FLV-Video, подключение по технологии ADSL.

Ход работы

1) Запустить программу Wireshark.

2) Через настройки интерфейса (Edit→Preferences…→User Interface→ Columns) сформировать колонки Number, Time, Packet Length. Сохранить настройки и перезапустить программу.

ВНИМАНИЕ! Для автоматической обработки данных через специальный файл Mathcad последовательность колонок должна быть именно такой, как написано выше.

3) В зависимости от номера бригады загрузить собранный дамп соответствующего типа (таблица 4.1).

Таблица 4.1

№ бриг	1	2	3	4	5	6	7	8
трафик	FTP	VoIP	WiFi	HTTP	Dial-Up	(Fast Ethernet	Strike	-Video
трафик	WiFi	(Fast Ethernet	VoIP	Strike (ADSL	Video (ADSL	Dial-Up	FTP	P

4) Поставить отображение времени, прошедшего с момента приёма последнего пакета (View→Time Display Format→Seconds Since Previous Packet).

5) Выделить одно направление дуплексного канала. Для этого необходимо задать фильтр ip.src == <IP-адрес отправителя>. В качестве адреса отправителя можно взять наиболее повторяющийся адрес в собранном дампе.

6) Для статистической обработки собранного дампа необходимо преобразовать его в текстовый файл. Для этого произвести печать данных в текстовый файл (File→Print…). Выбрать тип файла Plain text, поставить галочку в Output to file и справа задать путь для сохранения файла с данными, например C:\DATA.txt. Выбрать печать только отображённых пакетов (кнопка

[Displayed]). В группе настроек Packet Format убрать галочку с Packet details. Далее нажать кнопку [Print].

7) Открыть файл Statistics.mcd. В качестве аргумента функции READPRN ввести путь к сохранённому в предыдущем пункте файлу, например READPRN(«C:\DATA.txt»). Затем нажать клавишу F9.

8) Скопировать числовые характеристики и графики в отчёт.

9) Выполнить пункты 3–8 для дампа второго типа (таблица 4.1) и сравнить полученные статистические характеристики с характеристиками дампа первого типа.

10) Сделать выводы по полученным результатам статистического анализа.

Отчёт по лабораторной работе включает:

1) числовые характеристики исследуемого трафика;

2) гистограммы распределения и графики функций распределения вероятности времени прихода пакетов и их размера для двух типов трафика;

3) Выводы по результатам статистического анализа.

Контрольные вопросы

1) Что такое математическое ожидание? Что оно показывает?

2) Что такое дисперсия, среднее квадратическое отклонение? Каков их смысл?

3) Что называют модой случайной величины?

4) Что называют медианой случайной величины?

5) Что показывает функция распределения случайной величины?

6) Для чего строят гистограмму распределения?

7) Назовите основные параметры протоколов, влияющие на производительность сети.

8) Как влияет размер пакета на производительность сети?

9) Что такое квитирование?

10) Как влияет на производительность сети величина тайм-аута?

11) Как влияет на производительность сети размер окна неподтвержденных пакетов?

12) Для чего проводят статистический анализ трафика?

Листинг файла Statistics.mcd

На рисунках 4.2 – 4.4 представлена статистическая обработка времени прихода пакетов в файле Statistics.mcd, созданного в среде Mathcad.

На рисунках 4.5 – 4.7 показано как реализуется статистическая обработка размеров пакетов собранного дампа в файле Statistics.mcd.

DATA := READPRN("C:\DATA.txt")

i := 0.. rows(DATA) − 1

$V_i := DATA_{i,1}$

$U_i := DATA_{i,2}$

Время

V =

	0
0	3.336
1	0.014
2	0.014
3	3.832
4	0.35
5	0.049
6	0.089
7	0.033
8	0.034
9	0.033
10	0.038
11	0.033
12	0.033
13	0.033
14	0.052
15	0.033

Размер пакета

U =

	0
0	67
1	67
2	67
3	67
4	65
5	270
6	58
7	58
8	58
9	58
10	58
11	58
12	58
13	58
14	58
15	58

Время

Минимальное значение

min(V) = 0.013

Максимальное значение

maxV := max(V)

maxV = 11.242

Медиана

median(V) = 0.043

Мода

mode(V) = 0.033

Математическое ожидание

mean(V) = 0.059

Дисперсия

var(V) = 0.101

Рисунок 4.2 Файл Statistics.mcd

Среднеквадратическое отклонение

stdev(V) = 0.317

Гистограмма распределения

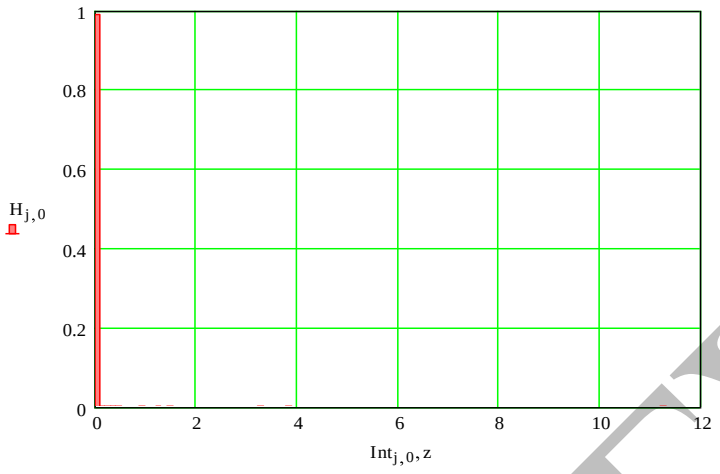
$n := 100$

$j := 0..n + 1$

$Int_j := \frac{maxV}{n} \cdot j$

$H := \frac{hist(Int, V)}{length(V)}$

$z := 0, 0.0000001 .. 0.01$



$n := 1000$

$j := 0..n + 1$

$Intv_j := \frac{maxV}{n} \cdot j$

$fv := hist(Intv, V)$

$j := 0..n$

$FV_j := \sum_{k=0}^{j} \frac{fv_k}{length(V)}$

Рисунок 4.3 Файл Statistics.mcd

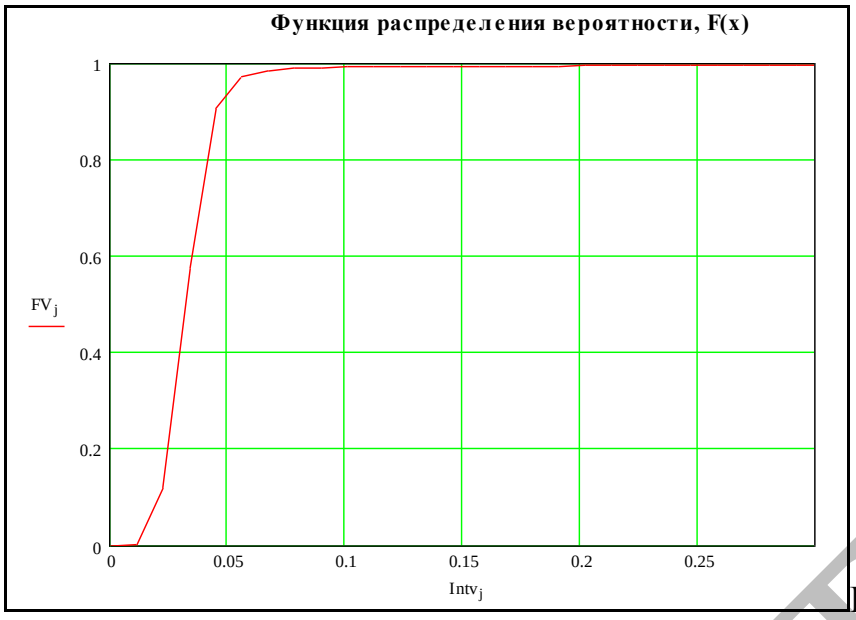


Рисунок 4.4 Файл Statistics.mcd

Размер пакета

Минимальное значени

min(U) = 58

Максимальное значени

maxU := max(U)

maxU = 270

Медиана

median(U) = 78

Мода

mode(U) = 76

Математическое ожидани

mean(U) = 79.544

Дисперсия

var(U) = 228.658

Рисунок 4.5 Файл Statistics.mcd

Среднеквадратическое отклонение

stdev(U) = 15.121

Гистограмма распределения

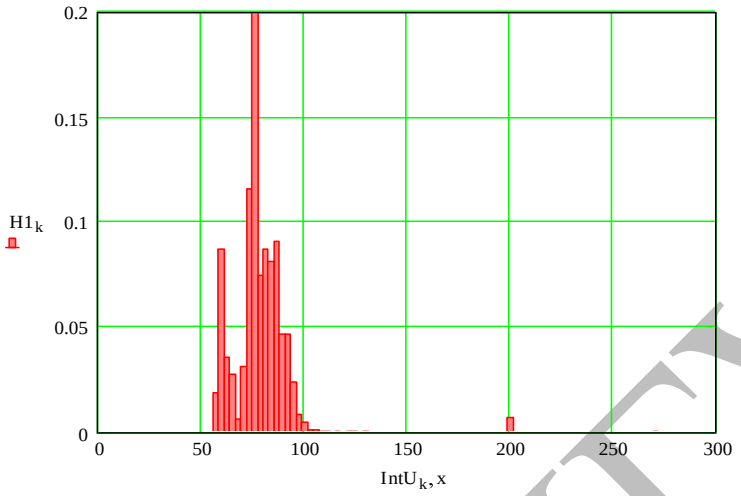
$m := 100$

$k := 0..m + 1$

$IntU_k := \frac{maxU}{m} \cdot k$

$H1 := \frac{hist(IntU, U)}{length(U)}$

$x := 0..1600$



$m := 1000$

$i := 0..m + 1$

$Intu_i := \frac{maxU}{m} \cdot i$

$fu := hist(Intu, U)$

$i := 0..m$

$FU_i := \sum_{k=0}^{i} \frac{fu_k}{length(U)}$

Рисунок 4.6 Файл Statistics.mcd

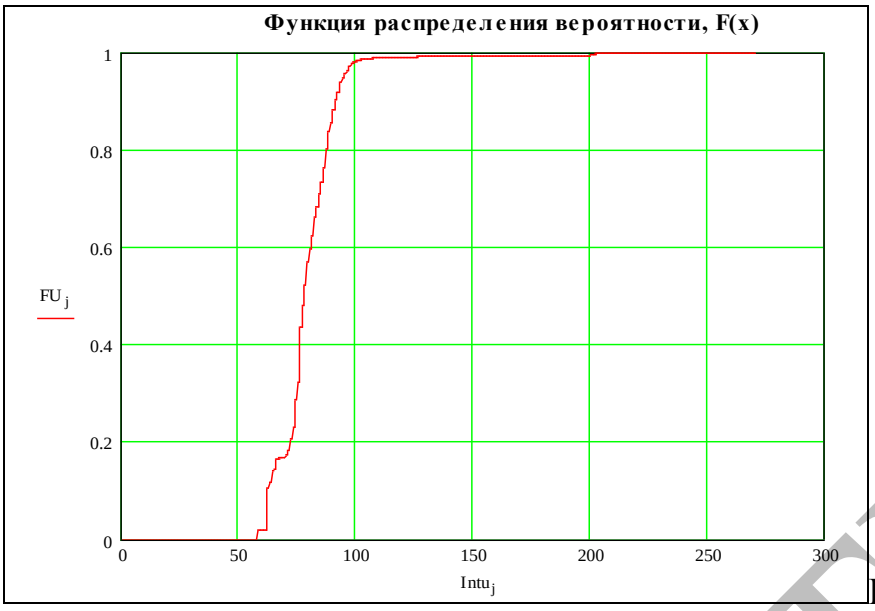


Рисунок 4.7 Файл Statistics.mcd