Семёнова Е.К.,
«Бизнес-информатика», 3 курс
Бардин А.К.,
доцент, к.э.н.
ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина»
Российская Федерация

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ОЦЕНКИ ТРАФФИКА НА УЗЛАХ ОС WINDOWS С ИСПОЛЬЗОВНИЕМ АНАЛИЗАТОРОВ ТРАФИКА

В статье рассматривается создание анализатора траффика как инструмента повышения эффективности анализа сетевого трафика для выявления проблем в различных сетевых протоколах.

This article describes the creating of traffic analyzer as an opportunity to improve the efficiency of network traffic analysis to identify problems in a variety of network protocols.

Использование компьютера сегодня практически всегда подразумевает использование Интернета, передачу данных между узлами системами. Поэтому контроль безопасности компьютера, отладка работы локальной сети, контроль исходящего трафика для оптимизации работы разделяемого подключения к Интернету — все эти задачи часто возникают на повестке дня как у системных администраторов, так и у простых пользователей. Для выявления проблем необходимо прибегнуть к сетевому мониторингу. Стандартные системные средства для осуществления этой задачи чаще либо отсутствуют вовсе, либо имеют недостаточный функционал. Полнофункциональный встроенный счетчик трафика впервые появился в Windows 8. Ранее, в версии Windows 7, существовала лишь инфраструктура сетевой диагностики Network Diagnostics Framework, позволяющая пользователям диагностировать и автоматически избавляться от проблем с сетью. В Windows 10 просмотреть использование сети можно на вкладке "Сеть и интернет" в меню "Параметры", нажав на "Использования данных".

Но, произвести подробный мониторинг для полноценного анализа трафика стандартными средствами системы Windows невозможно. Поэтому для решения этой задачи существуют различные утилиты, называемые анализаторами или снифферами. Большая часть из них является специализированными, направленными на решение узкой области задач,

либо многофункциональными, предоставляющими пользователю широкий выбор инструментов.

В качестве основы предлагаемого анализатора рассмотрен анализатор, описанный в статье «Программный анализ трафика на примере ОС Linux Ubuntu 13.04» Сборника Материалов VI Международного Форума. Главными его недостатками является недостаточное количество обрабатываемых протоколов, а также отсутствие полноценного интерфейса. Для устранения указанных недостатков предлагается универсальное решение для ОС Windiws 7 и выше – сниффер с базовым функционалом, который может найти применение в любой сфере, где необходим мониторинг трафика.

При реализации задачи был выбран язык программирования C#, библиотеки с PcapDotNet и WinPcap, представляющие собой сборник библиотек для взаимодействия с сетевыми адаптерами. Особенностью WinPcap является поддержка перехвата сетевых пакетов, минуя стеки протоколов, что исключает пропуск пакетов. Приложение надежно фильтрует сетевые пакеты, сводя к минимуму сетевые уязвимости.

Структура и размеры пакета в каждой сети зависят от используемого протокола, поэтому важным аспектом является понимание организации передачи данных в соответствии с протоколом. Извлечение информации в предлагаемой программе производится с учетом особенностей текущего протокола. Программа анализирует трафик для протоколов TCP, UDP, HIP, ICMP и IGMP. Пакеты прочих протоколов, распознаваемые библиотеками PcapDotNet и WinPcap, также отражены программой, но без возможности настроить фильтрацию по каждому из них.

Алгоритм обработки имеет древовидную структуру, построенную на условиях, что исключает лишнюю обработку пакетов (рис. 1).

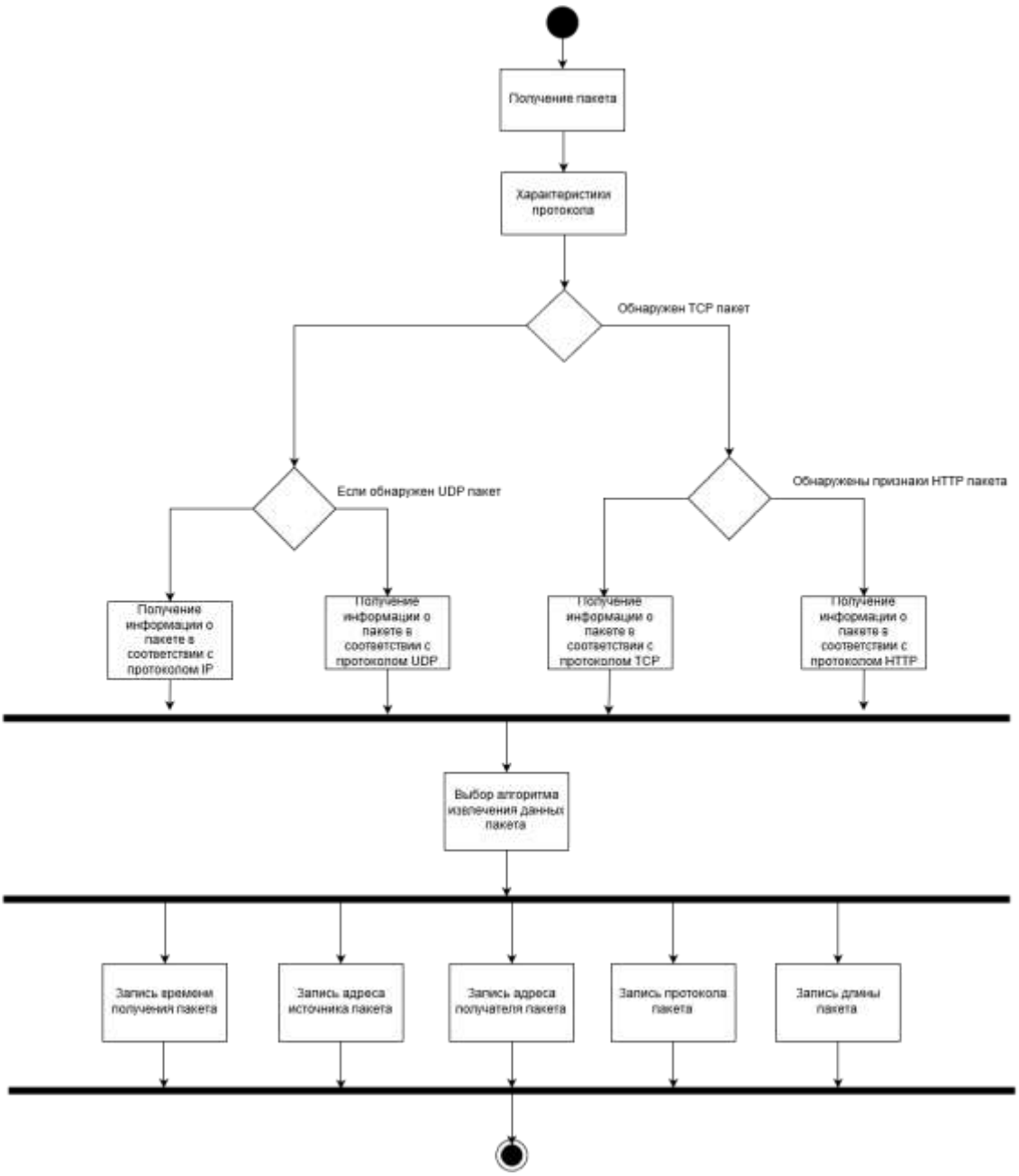

Рисунок 1 – Диаграмма обработки пакета входящего и исходящего трафика в соответствии с его протоколом

Программа определяет протокол передачи пакета и, исходя из этого, применяются соответствующие им методы библиотек, извлекающие данные. Остается лишь произвести их запись и в удобном виде предоставить пользователю. Следует отметить, что вывод пакетов происходит по таймеру, с указанием времени. Полная диаграмма работы приложения для анализа и управления трафиком в OS Windows представлена на рисунке 2.

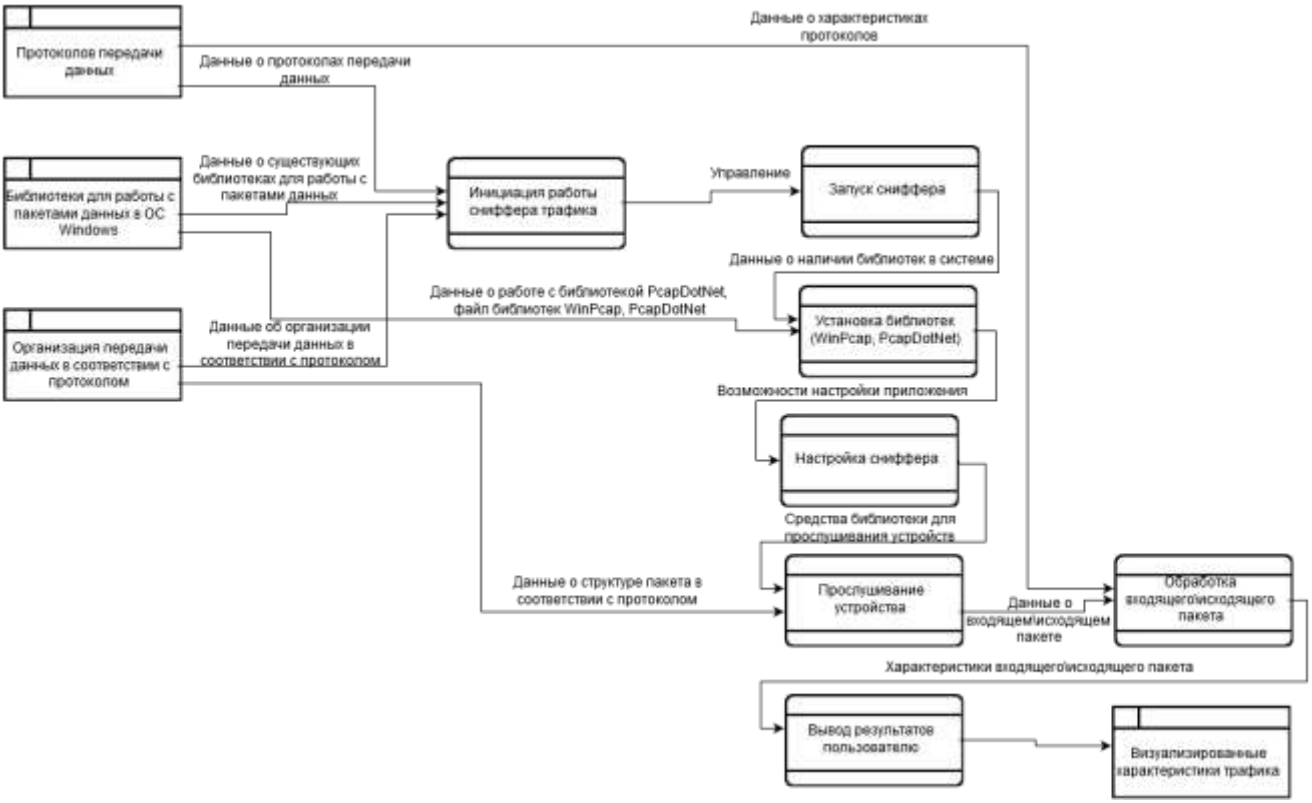

Рисунок 2 – Диаграмма работы приложения анализа и управления трафиком в OS Windows

Работа сниффера происходит следующим образом: при первом запуске программа предлагает установить необходимую для работы библиотеку. После ее установки пользователю будет представлена главная форма приложения (рис.3), в которой необходимо произвести некоторые простые настройки: выбрать сетевое устройство для прослушки и установить фильтрацию протоколов.

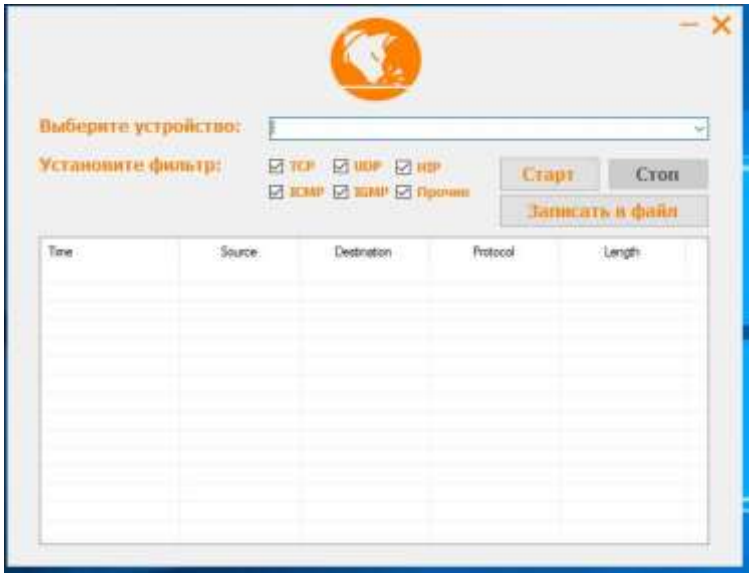

Рисунок 3 – Главная форма сниффера траффика

Дальнейшее прослушивание и обработку пакетов значительно упрощает использование библиотек.

Благодаря простоте реализации, пользователю не составит большого труда разобраться в работе приложения, а разработчику – в исходном коде, что позволяет дополнять, модифицировать его в зависимости от поставленной задачи.

Список использованных источников:

1. Грибков М.Е., Бардин А.К. Программный анализ трафика на примере ОС Linux Ubuntu 13.04 [Статья] / Грибков М.Е., Бардин А.К. // Информационное общество: современное состояние и перспективы развития: сборник материалов VI международного форума. – Краснодар: КубГАУ, 2016. – С. 170-175.

2. Перехват сетевых данных [Электр. ресурс]; Режим доступа: http://alex-shtilev.narod.ru/diplom/glava16.html свободный, загл. с экрана, - Яз. Рус.

3. Руководство по TCP/IP для начинающих. [Электр. Ресурс] Режим доступа: http://www.codenet.ru/webmast/tcpip.php свободный, загл. с экрана, - Яз. рус.