

УДК 004.056

ИССЛЕДОВАНИЕ МЕТОДА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ НА БАЗЕ ИНТЕРФЕЙСА USB

Варавка А.В., Цололо С.А.

ГВУЗ «Донецкий национальный технический университет», г. Донецк

Кафедра компьютерной инженерии

E-mail: antosha90@yandex.ru

Аннотация

Варавка А.В., Цололо С.А. Исследование метода информационной безопасности в компьютерных системах на базе интерфейса USB. Выполнен анализ особенностей архитектуры, принципов работы и взаимодействия компонентов USB. Предложен метод информационной безопасности в компьютерных системах на базе интерфейса USB. Рассмотрен пример реализации предложенного метода.

Введение

Шина USB (Universal Serial Bus – универсальная последовательная шина) является промышленным стандартом расширения архитектуры персонального компьютера, ориентированным на интеграцию с телефонией и устройствами бытовой электроники. Спецификация периферийной шины USB была разработана лидерами компьютерной и телекоммуникационной промышленности – Compaq, DEC, IBM, Intel, Microsoft, NEC и Northern Telecom – для подключения компьютерной периферии вне корпуса рабочей станции по стандарту Plug-and-Play, в результате чего отсутствует необходимость в установке дополнительных плат в слоты расширения и переконфигурировании системы. Шина USB позволяет одновременно подключать последовательно до 127 устройств, которые могут быть как дополнительными компонентами рабочей станции (внешние накопители, устройства ввода, мобильные терминалы и прочее), так и хабами (узлами) – устройствами, через которые подключаются оконечные дополнительные компоненты [1].

Для исследований выбран стандарт USB 2.0, который позволяет производить обмен информацией с периферийными устройствами в трех режимах: Low Speed (низкая скорость, до 1,5 Мбит/с), Full Speed (стандартная скорость, до 12 Мбит/с), High Speed (высокая скорость, до 480 Мбит/с). Появившийся в 2010 году стандарт USB 3.0 все еще не входит в стандартное оснащение современных чипсетов и пока не получил широкого распространения. Стандарт USB 3.0 полностью физически и логически совместим с USB 2.0, предельной пропускной способности в 480 Мбит/с достаточно для удовлетворения потребностей всех применений в полной мере, поэтому предложенная разработка сохранит свою актуальность и работоспособность при будущем переходе на следующий стандарт (взято с источника 2).

В данной работе авторами предлагается метод информационной безопасности в компьютерных системах. В основе метода лежит мониторинг устройств, подключаемых по интерфейсу USB.

Актуальность предложенного подхода заключается в необходимости реализации контроля обмена потоков данных между рабочими станциями и пользователем для обеспечения максимальной конфиденциальности информации.

Научная новизна работы заключается в разработке программы-мониторинга устройств, подключаемых по интерфейсу USB.

Архитектура шины USB

Архитектура и основные параметры шины USB определяются возложенными на нее задачами. Физическая топология шины USB, изображенная на рисунке 1, имеет следующие основные особенности:

- шина обеспечивает подключение USB - устройств к хосту USB;
- физическое соединение устройств между собой осуществляется по топологии многоярусной звезды;
- центром каждой звезды является хаб;
- каждый кабельный сегмент соединяет между собой две точки: хост с хабом или функцией, хаб с функцией или другим хабом.

Хост-контроллер (Host Controller) — это главный контроллер, который входит в состав системного блока компьютера и управляет работой всех устройств на шине USB.

На шине USB допускается наличие только одного хоста. Системный блок АТ-совместимого персонального компьютера может содержать от одного до трех хост-контроллеров, каждый из которых управляет отдельной шиной USB.

Устройство (Device) USB может быть хабом или функцией.

Хаб (Hub) — это устройство, которое обеспечивает дополнительные точки подключения к шине USB.

Каждый хаб имеет один восходящий порт (Upstream Port), предназначенный для подключения к хабу верхнего уровня, и несколько нисходящих портов (Downstream Ports), предназначенных для подключения функций или хабов нижнего уровня.

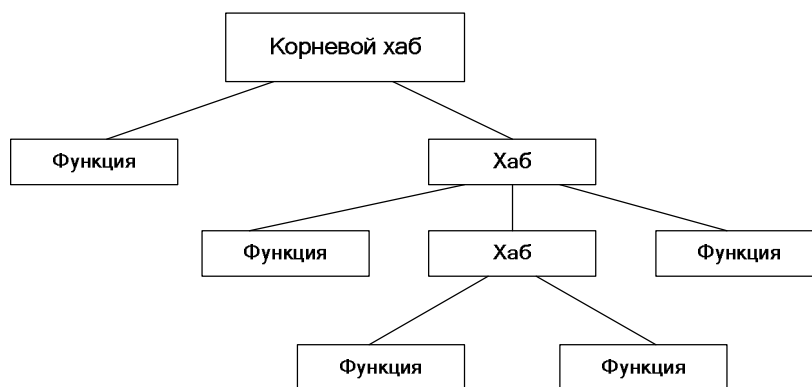


Рисунок 1 – Физическая топология шины USB

Хаб может иметь собственный источник питания (Self-powered Hub) или получать питание от шины USB (Bus-powered Hub). Хаб управляет работой нисходящих портов, осуществляет контроль подключения и отключения устройств. Через порты хаб управляет электропитанием устройств, не имеющих собственных источников энергии.

Корневой хаб (Root Hub) — это хаб, который входит в состав хост-контроллера.

Функция (Function) — это периферийное устройство или отдельный блок периферийного устройства, способный передавать и принимать информацию по шине USB.

Составное устройство (Compound Device) — это периферийное устройство со встроенным хабом.

Различают три уровня взаимодействия хоста с физическим устройством:

- на верхнем уровне (уровне функции) между собой взаимодействуют клиентская программа и функция;
- на среднем уровне (уровне устройства) взаимодействуют системное программное обеспечение и логическое устройство USB;
- на нижнем уровне (уровне интерфейса шины USB) хост-контроллер взаимодействует с USB -интерфейсом устройства.

Используемая на среднем уровне взаимодействия логическая топология шины USB (рисунок 2) гораздо проще физической: хост обменивается информацией с логическими устройствами таким образом, что точка подключения устройства не имеет значения, как если бы все устройства были подключены к корневому хабу.

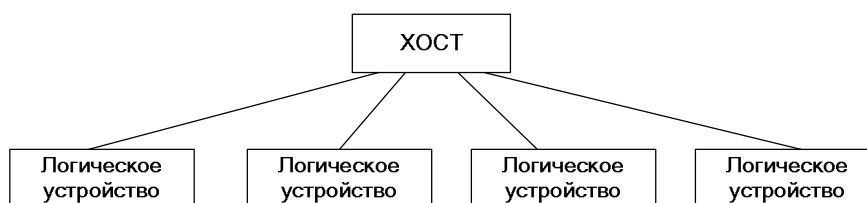


Рисунок 2 – Логическая топология шины USB

Режимы и модели передачи данных

Пропускная способность шины USB, соответствующей спецификации 1.1, составляет 12 Мбит/с (1,5 Мбайт/с). Полоса пропускания шины делится между всеми устройствами, подключенными к шине.

Шина USB имеет два режима передачи: в полноскоростном (full-speed) режиме скорость передачи составляет 12 Мбит/с, в низкоскоростном (low-speed) — 1,5 Мбит/с. Полноскоростной режим используется принтерами, сканерами, видекамерами и другими устройствами, передающими больше объемы информации. Низкоскоростной режим предназначен для упрощения конструкции и снижения себестоимости устройств, обменивающихся с компьютером небольшими порциями данных — мыши, джойстика и т. п. Устройство, использующее полную скорость передачи, именуется полноскоростным (Full-speed Device), а устройство, использующее пониженную скорость — низкоскоростным (Low-speed Device).

Вся информация передается по шине USB в виде пакетов. Каждый пакет начинается с поля синхронизации (SYNC), за которым следует идентификатор пакета (PID). Идентификатор пакета состоит из четырехразрядного кода типа пакета и четырехразрядного контрольного поля, каждый разряд которого является инверсией соответствующего разряда кода типа пакета (код пакета и контрольное поле комплементарны).

Все транзакции на шине USB выполняются под управлением хост контроллера. Передача данных возможна только по запросам хоста: периферийные устройства не могут выдать на шину какую-либо информацию по собственной инициативе, не могут самостоятельно посылать запросы прерываний.

Программа- мониторинг устройств, подключаемых по интерфейсу USB

Результатом данного исследования является написание программного обеспечения, с помощью которого можно определить параметры и характеристики устройств, которые подключены к шине USB персонального компьютера. Алгоритм работы программы изображен на рисунке 3. Результаты программного обеспечения представлены на рисунке 4 и 5.

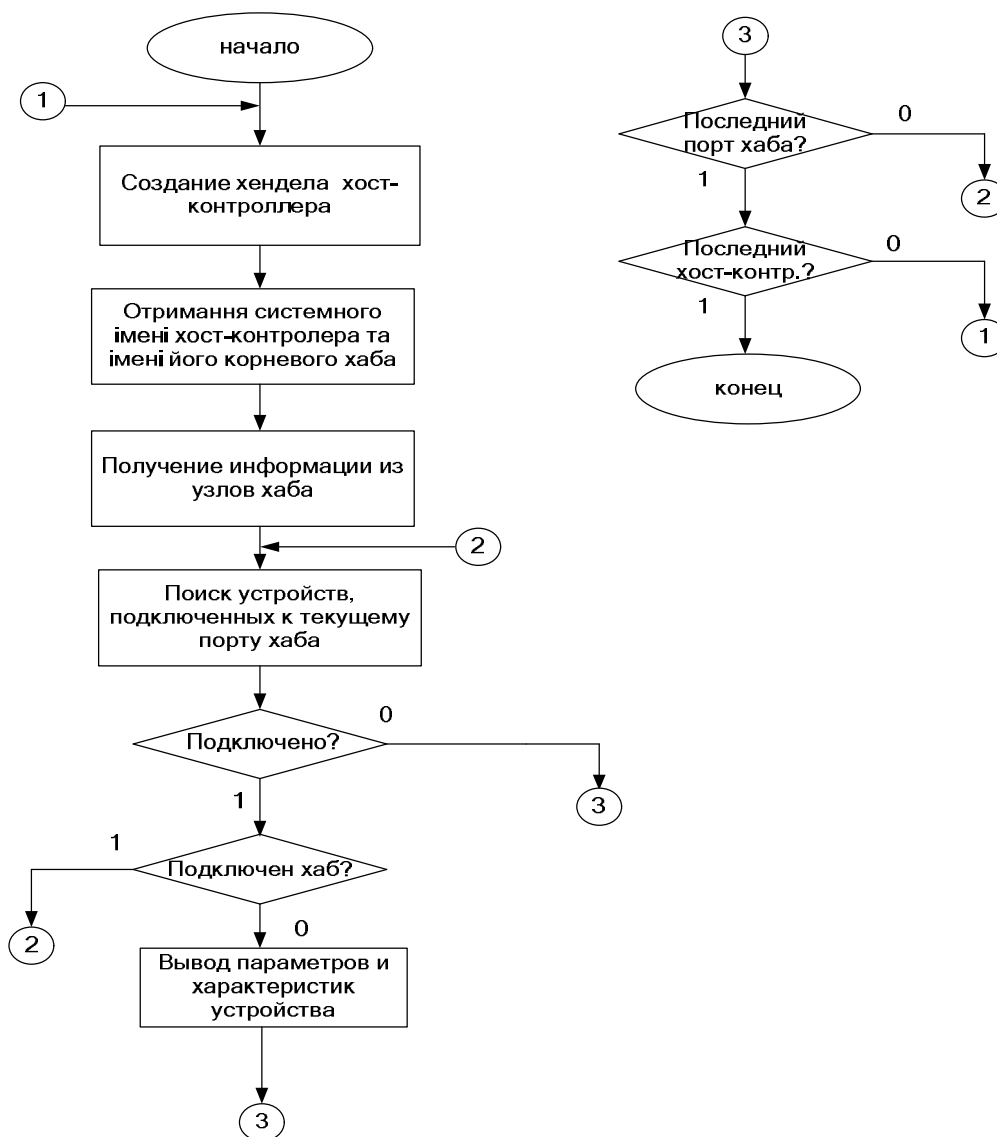


Рисунок 3 - Алгоритм работы программы-мониторинга USB-устройств

Программа мониторинга USB-устройств обнаруживает хост-контроллеры, которые установлены в компьютере, находит хабы и их порты, потом сканирует их на наличие подключенных устройств. Если устройство найдено, тогда формируются запросы на получение информации стандартных дескрипторов устройств, которые описываются в разделе 4. Сначала получаем информацию дескриптора устройства, потом отправляется

запрос на получение дескриптора конфигурации. Размер стандартного дескриптора конфигурации всегда составляет 9 байт, а код типа дескриптора имеет значение 2. По запросу «Получить стандартный дескриптор конфигурации» каждое устройство выдает не только дескриптор конфигурации, но и все имеющиеся дескрипторы интерфейсов и конечных точек. Поэтому, если за какой-то причиной нельзя получить дескриптор конфигурации информация дескрипторов строки, конечной точки, интерфейса будет недоступной

```
Host Controller \\.\HCD0 found. System name is {36FC9E60-C465-11CF-8056-444553540000}\0003
  Port[1] = No device connected
  Port[2] = No device connected

Host Controller \\.\HCD1 found. System name is {36FC9E60-C465-11CF-8056-444553540000}\0002
  Port[1] = No device connected
  Port[2] = No device connected

Host Controller \\.\HCD2 found. System name is {36FC9E60-C465-11CF-8056-444553540000}\0001
  Port[1] = No device connected
  Port[2] = No device connected

Host Controller \\.\HCD3 found. System name is {36FC9E60-C465-11CF-8056-444553540000}\0000
  Port[1] = No device connected
  Port[2] = No device connected
  Port[3] = No device connected
  Port[4] = I/O device connected

Device Descriptor
  bLength          12
  bDescriptorType  01
  bcdUSB           0200
  bDeviceClass     00
  bDeviceSubClass  00
  bDeviceProtocol  00
  bMaxEPSize       40
  wVendorID        058F
  wProductID       6387
  wDeviceID        0141
  iManufacturer    01 = JetFlash
  iProduct          02 = Mass Storage Device
  iSerialNumber    03 = ZNB8C56U
  bNumConfigurations 01
```

Рисунок 4 - Результаты работы программы-мониторинга USB-устройств

Выводы

В результате анализа архитектуры и взаимодействия компонентов USB был предложен метод информационной безопасности на базе интерфейса USB, а также приведены результаты программы-мониторинга устройств USB.

Реализация предложенного метода может быть полезна в общественных, частных или государственных предприятиях для обеспечения конфиденциальности данных внутри компьютерной системы предприятия.

Литература

1. Агуров П. В. Интерфейс USB. Практика использования и программирования. – СПб: БХВ-Петербург, 2004. – 576 с. – ISBN 5-94157-202-6
2. Варавка А.В., Цололо С.А., Демеш Н.С. Исследование алгоритма обеспечения информационной безопасности в компьютерных системах предприятий на базе интерфейса USB. – ГБУЗ ДонНТУ, 2011 г., «Информатика и компьютерные технологии 2011».
3. Скотт Мюллер. Модернизация и ремонт ПК (глава 15 – Последовательный, параллельный и другие интерфейсы ввода/вывода – USB) = Upgrading and Repairing PCs. – 17 изд. – М.: «Вильямс», 2007. – С. 1016-1026. – ISBN 0-7897-3404-4

4. Интересное о USB [электронный ресурс]. – Режим доступа: <http://hi-tech.mail.ru/articles/item/1896/>
5. Don Anderson. Universal Serial Bus System Architecture [электронный ресурс]. – Режим доступа: http://interface.centraltreasure.com/files/pdf/Hardware_USB_System_Architecture_pdf.pdf