УДК 004.056

ИССЛЕДОВАНИЕ АЛГОРИТМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ ПРЕДПРИЯТИЙ НА БАЗЕ ИНТЕРФЕЙСА USB

Варавка А.В., Цололо С.А., Демеш Н.С.
Донецкий национальный технический университет,
кафедра компьютерной инженерии
antosha90@yandex.ru

Выполнен анализ особенностей архитектуры, принципов работы и взаимодействия компонентов USB. Предложен алгоритм обеспечения информационной безопасности в компьютерных системах предприятий на базе интерфейса USB. Рассмотрены особенности путей реализации предложенного алгоритма.

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.

В работе авторами предлагается алгоритм обеспечения информационной безопасности в компьютерной сети предприятия. В основе алгоритма лежит контроль информационных потоков между рабочими станциями сотрудников и внешними накопителями, подключаемыми по интерфейсу USB.

Актуальность предложенного подхода заключается в необходимости реализации контроля за внутренними и внешними потоками данных предприятия для обеспечения максимальной конфиденциальности внутрикорпоративной информации.

Научная новизна работы заключается в разработке интеллектуального алгоритма фильтрации информационных потоков, которые передаются с/на USB-накопители. Алгоритм фильтрации предоставляет возможностью вычленения заданной информации по широкому набору параметров (имя процесса или файла, маска данных, дата/время записи/чтения и другие).

Практическая ценность предложенного алгоритма заключается в разработке клиент-серверной программы-разведчика, которая обеспечивает контроль, управление и сбор статистики по подключаемым к рабочим станциям сотрудников USB-накопителям, а также содержанию информационных потоков, идущих с/на них.

Архитектура и взаимодействие компонентов USB

Стандарт USB всех версий (далее просто USB) обеспечивает обмен данными между рабочей станцией (хостом) и множеством одновременно доступных периферийных устройств. Распределение пропускной способности шины между подключенными устройствами планируется хостом и реализуется им с помощью посылки маркеров. Шина позволяет подключать, конфигурировать, использовать и отключать устройства во время работы хоста и самих устройств, то есть реализует динамическое («горячее») подключение и отключение. Устройства USB могут являться хабами, «функциями» или их комбинацией. Хаб обеспечивает дополнительные точки подключения устройств к шине. «Функции» USB предоставляют системе дополнительные возможности – подключение мыши, игрового джойстика, акустической системы с цифровым интерфейсом и так далее. Работой всей системы USB управляет хост-контроллер. являющийся программно-аппаратной подсистемой хоста [2].

«Функции» представляют собой устройства USB, способные принимать или передавать данные или управляющую информацию по шине. Физически в одном корпусе может быть несколько «функций» со встроенным хабом, который обеспечивает их подключение к одному порту. Каждая «функция» предоставляет конфигурационную информацию, описывающую его возможности и требования к ресурсам. Перед использованием функция должна быть сконфигурирована хостом – ей должна быть выделена полоса в канале, а также выбраны специфические опции конфигурации.

Хаб – ключевой элемент системы Plug-and-Play в архитектуре USB. Хаб является кабельным концентратором, точки подключения называются портами хаба. Каждый хаб преобразует одну точку подключения в их множество. Архитектура подразумевает возможность соединения нескольких хабов.

Структурно система USB разделяется на три уровня с определенными правилами взаимодействия. Устройство USB делится на интерфейсную часть, часть устройства и функциональную часть. Хост также разделяется на три части – интерфейсную, системную и ПО устройства [3, 4]. Каждая часть отвечает только за определенный круг задач, взаимодействие между ними показано на рис. 1.

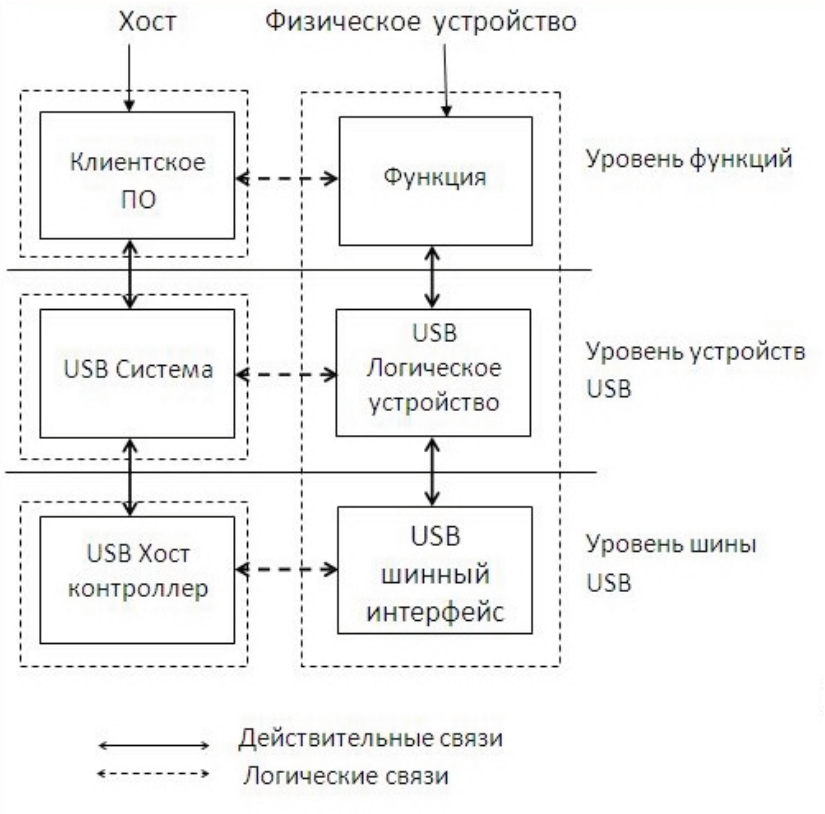

Рисунок 1. Взаимодействие компонентов USB

Алгоритм обеспечения информационной безопасности на базе интерфейса USB

Каждый пользователь современного персонального компьютера имеет возможность хранить и передавать информацию с помощью USB-накопителей (флэш-память). Стоимость таких устройств на компьютерном рынке составляет около 10 долларов в зависимости от емкости. В связи с довольно низкой стоимостью, а также достаточно гибким и удобным использованием флеш-памяти большинство пользователей и работников предприятий выбирают именно данный способ хранения и передачи информации.

С точки зрения корпоративной безопасности и обеспечения конфиденциальности внутренних данных часто необходимо вести контроль внутрикорпоративных информационных потоков. Поэтому авторами предлагается описание алгоритма наблюдения за рабочими станциями сотрудников какой-либо организации или предприятия. Конечной целью работы алгоритма является контроль информации, которая перемещается сотрудниками между жесткими дисками рабочих станций и внешними USB-носителями.

Предлагаемый алгоритм наблюдения реализуется программой-разведчиком, которая будет отслеживать работу всех накопителей, подключаемых к рабочим станциям сотрудников через шину USB (рис. 2).

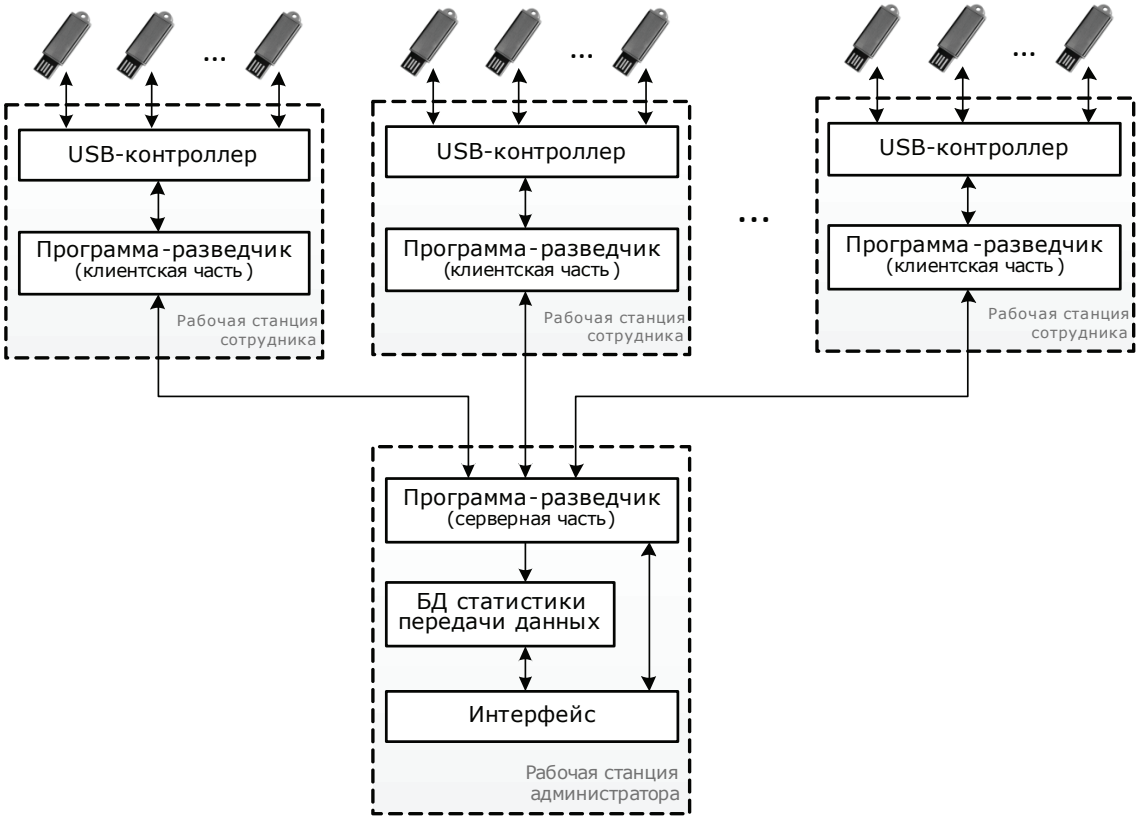

Рисунок 2. Принцип взаимодействия программ-разведчиков с контроллерами шины USB и компьютером администратора

Как видно из рис. 2, программа-разведчик структурно состоит из двух частей – клиентской и серверной, которые взаимодействуют друг с другом по локальной сети.

Клиентская часть запускается на локальной рабочей станции сотрудника и выполняет следующие функции:

1. Автозапуск программы-разведчика при старте операционной системы.
2. Определение типов подключаемых USB-устройств, а также группы параметров, характеризующих устройство (производитель, модель, серийный номер).
3. Контроль запросов на чтение/запись информации, возможность вычленения заданной информации по имени процесса или файла, маске или содержимому.

4. Определение MAC- и IP-адреса рабочей станции.
5. Передача собранной информации на сервер, объем пакета информации настраивается.
6. Функционирование в скрытом режиме (в виде службы).

Серверная часть программы-разведчика запускается на рабочей станции администратора и выполняется следующие основные функции.

1. Проверка работоспособности и полное удаленное управление всеми программами-клиентами.
2. Сбор и накопление информации от программ-клиентов.
3. Пакетная настройка всех подключенных клиентов.
4. Предоставление пользовательского интерфейса к накопленной информации.

Выводы

В результате анализа архитектуры и взаимодействия компонентов USB был предложен алгоритм обеспечения информационной безопасности на базе интерфейса USB, а также изложен общий принцип работы программы-разведчика.

Реализация предложенного алгоритма может быть полезна в общественных, частных или государственных предприятиях как для обеспечения контроля конфиденциальности данных внутри компьютерной системы предприятия, так и для предотвращения утечек корпоративной информации за пределы предприятия.

Литература

[1] Агуров П. В. Интерфейс USB. Практика использования и программирования. – СПб: БХВ-Петербург,2004. – 576 с. – ISBN 5-94157-202-6

[2] 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

[3] Интересное о USB [электронный ресурс]. – Режим доступа: http://hi-tech.mail.ru/articles/item/1896/

[4] Don Anderson. Universal Serial Bus System Architecture [электронный ресурс]. – Режим доступа: http://interface.centraltreasure.com/files/pdf/Hardware_USB_ System_Architecture_pdf.pdf