В результате можно получить следующий код Хэмминга V(9,3):

$$\begin{pmatrix} 0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&1&0&1&1&1 \\ 0&1&1&0&0&1&0&0&1 \\ 0&0&1&0&1&1&1&1&0 \\ 1&0&0&1&0&0&1&0&1 \\ 1&1&0&1&1&0&0&1&0 \\ 1&1&1&1&0&1&1&0&0 \\ 1&0&1&1&1&1&0&1&1 \end{pmatrix}$$

Расстояние кода равно 4. Поэтому код может исправлять одну ошибку и обнаруживать 3 и менее ошибок. Было создано нормально расположение для исправления единичных ошибок, вычислена проверочная матрица и составлена таблица синдромов образующих элементов каждого смежного класса. С помощью генератора случайных чисел в каждом кодовом слове была смоделирована ошибка в одном из регистров, затем с помощью таблицы синдромов выполнена декодирование с исправлением ошибок.

Заключение. Таким образом, рассмотрен принцип построения блоковых кодов Хэмминга на основе порождающей матрицы и порождающего многочлена. Подробно рассмотрим алгоритм декодирование на основе синдромов.

Литература:

1. Библиотека по математике: [Электронный ресурс]. – Режим доступа: http://mathemlib.ru/books/item/f00/s00/z0000023/index.shtml - Дата доступа: 20.02.2017.
2. Институт дистанционного образования: [Электронный ресурс]. – Режим доступа: https://ido.tsu.ru/iop_res1/kodi/index.php-mod=menu&m=2.htm - Дата доступа: 22.02.2017.

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПРИ РАБОТЕ В КОМПЬЮТЕРНОМ КЛАССЕ ВОЕННОЙ КАФЕДРЫ ВГУ ИМЕНИ П.М. МАШЕРОВА

Романюк А.А.,
студент 4 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – Станкевич С.М.

Предотвращение несанкционированного доступа является одной из основных проблем защиты информации. Все популярные операционные системы содержат различные подсистемы защиты от несанкционированного доступа. Например, при запуске сеанса работы в операционных системах семейства MS Windows выполняется аутентификация пользователей.

Выпускаемые производителями программного обеспечения пакеты обновлений и исправлений программных продуктов объективно несколько отстают от информации об обнаруживаемых уязвимостях. Поэтому в дополнение к стандартным средствам защиты необходимо использование специальных средств ограничения или разграничения доступа [1].

Целью настоящей работы является разработка программного средства для защиты персональных компьютеров от несанкционированного подключения USB-устройств на военной кафедре ВГУ имени П.М. Машерова.

Материал и методы. При разработке программного средства для защиты USB-портов от несанкционированного доступа использовался пакет Microsoft Visual Studio 2015. Пакет представляет собой набор инструментов для создания программного обеспечения: планирование разработки, разработка пользовательского интерфейса, написание кода, тестирование, отладка, анализ качества кода и производительности, развертывания в средах клиентов и сбора данных телеметрии по использованию. Все инструменты доступны в интегрированной среде разработки (IDE) Visual Studio. По умолчанию VisualStudio обеспечивает поддержку языков программирования C#, C и C++, JavaScript, F# и VisualBasic [2].

В качестве языка программирования в данной работе использовался C#.

В процессе разработки программного средства защиты персональных компьютеров от несанкционированного доступа решались следующие задачи:

1. Изучение принципов построения системы безопасности компьютерного класса военной кафедры.
2. Изучение принципы функционирования шины USB.
3. Определение набора групп пользователей и системных разрешений для работы с реестром операционной системы в контексте подключения USB-устройств.
4. Проектирование и программирование инструмента для предотвращения несанкционированного подключения USB-устройств к персональному компьютеру.

При запуске программы появляется окно. Пользователь должен вставить USB-устройство в порт. Когда система обнаруживает факт подключения устройства, программа проверяет, входит ли серийный номер подключенного устройства в список разрешенных.

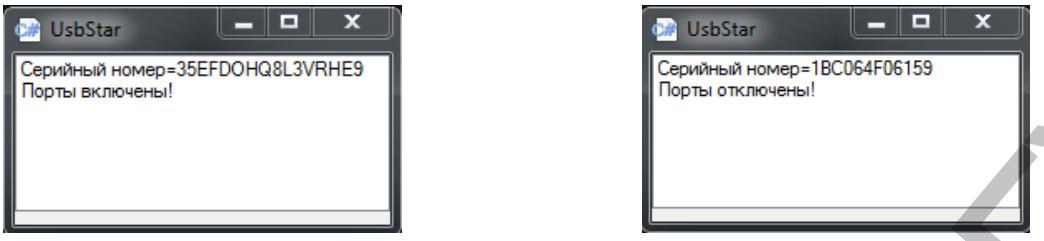

Рисунок 1 – Сообщения о подключении и отключении портов

Если доступ разрешен, в окне программы появится сообщение «Порты включены!» и будет показан серийный номер устройства (рис. 1). Если доступ запрещен, в окне программы появится сообщение «Порты выключены!» и снова будет показан серийный номер устройства (см. рис. 1). После отключения и извлечения USB-устройства порты будут включены.

Заключение. В результате выполнения работы были:

– изучены принципы построения системы безопасности при работе в компьютерном классе;

– изучены принципы функционирования шины USB;

– определены наборы групп пользователей и системных разрешений для работы с реестром ОС в контексте подключения USB-устройств;

– разработано программное обеспечение для предотвращения несанкционированного подключения USB-устройств к персональному компьютеру.

Литература

1. Щесняк, Е.Л. Комплексная безопасность высшего учебного заведения / Е.Л. Щесняк, В. Г. Плющиков, В.С. Побыванец.– Москва: Российский университет дружбы народов, 2011. — 768 с.
2. Интегрированная среда разработки Visual Studio [Электронный ресурс]. - 2017. - Режим доступа: https://msdn.microsoft.com/ru-ru/library/dn762121.aspx. -Дата доступа: 10.02.2017.

РЕАЛИЗАЦИЯ МЕТОДА ПЕРЕМЕННЫХ НАПРАВЛЕНИЙ В КОНТЕКСТЕ АЛГОРИТМОВ РАСПАРАЛЛЕЛИВАНИЯ

Савостеенко Е.В.,
магистрант 6 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – Маркова Л.В., канд. физ.-мат. наук, доцент

Инновационное развитие общества сегодня напрямую связано с решением задач, требующих большого объема весьма сложных вычислений. Нет ни одной области науки и техники, в которой бы не ставились задачи математического моделирования. Это задачи ядерного синтеза, генной инженерии, тепло и массопереноса, экологических и метеопрогнозов, изучения человека, создания роботов и т.д. В основе вычислений каждой задачи лежат алгоритмы, важнейшим критерием разработки которых является их эффективность [1].

Цель исследования – показать возможность повышения эффективности решения задачи в зависимости от программной реализации вычислительного алгоритма.

Материал и методы. Материалом исследования была выбрана двумерная квазилинейная задача теплопроводности. Основные методы исследования – системный подход, анализ литературы, методы ООП и параллельных вычислений, вычислительный эксперимент.

Результаты и их обсуждение. Большое количество программного обеспечения, написанного ранее для последовательной (однопроцессорной) вычислительной техники, не обладает необходимым запасом параллелизма и попытки его распараллеливания на уровне распараллеливания отдельных циклов, как правило, не приводят к хорошим результатам. Производительность кода остается низкой.

Другим подходом к разработке параллельных программ является использование модели программирования с распараллеливанием данных, когда в последовательный код вставляются директивы компилятору и распараллеливание происходит на автоматическом уровне. Если программа логически простая и обладает ресурсом параллелизма, этот подход может дать хорошие результаты. Однако рекордных результатов удается получить только при использовании знаний программиста о структуре алгоритма и управлении вручную потоком данных. Это достигается при использовании стиля программирования с передачей сообщений [3].