УДК 004.056.5

АППАРАТНО ПРОГРАММНЫЙ КОМПЛЕКС ФИЗИЧЕСКОГО РАЗГРАНИЧЕНИЯ ДОСТУПА ПЭВМ

МАРМУЗЕВИЧ М. А., БУНЕВИЧ М. А.

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

E-mail: marmuzevich@bsuir.by, mike_box@bk.ru

Аннотация. Одним из основных путей решения технических, социальных и экономических задач является использование информационных технологий. Целью данной работы была разработка аппаратно программного комплекса для защиты и ограничения доступа к информации путём дополнительной идентификации пользователя в системе. По результатам проведённых исследований предложен алгоритм работы устройства и разработан прототип аппаратно программного комплекса физического разграничения доступа ПЭВМ. Данный комплекс может быть использован в ПЭВМ различных конфигураций.

Abstract. One of the main ways to solve technical, social and economic problems it the use of information technologies. The purpose of this work was to develop a hardware and software complex for protecting and restricting access to service information by additional user identification in the system. Based on the results of the research, an algorithm for the operation of the device was proposed and a prototype of a hardware-software complex for physical access control of a PC was developed. This complex can be used in a personal computer of various configurations.

Современный этап развития информационных технологий характеризуется расширением сферы применения вычислительной техники и высоким уровнем использования автоматизированных систем управления и обработки информации. Наибольшую опасность с точки зрения утечки информации представляет утечка данных с носителей информации. Целью разграничения доступа к информации в первую очередь является предотвращение реализации угрозы нарушения конфиденциальности или несанкционированного доступа к информации. Можно выделить следующие виды несанкционированного доступа:

– доступ к носителям информации;
– локальный доступ к отдельным персональным компьютерам;
– локальный доступ к ресурсам сети;
– удаленный доступ к отдельным компьютерам или ресурсам сети.

Для первых двух видов важное значение имеют организационно-режимные меры доступа к машинным носителям информации такие, как пропускной режим, охрана, замки на дверях. В тоже время достаточно сложно организовать контроль за действиями пользователя, работающего с конфиденциальными файлами на ПЭВМ, что может дать ему возможность беспрепятственного доступа к информации на других жёстких дисках. Путём атак на средства аутентификации с целью получения пароля или других данных для идентификации в системе под другим логином возможно получить доступ или уничтожить ценную информацию.

Целью данной работы была разработка аппаратно программного комплекса, для защиты и ограничения доступа к носителям информации без дополнительной идентификации пользователя в системе. При включении компьютера Basic Input/Output System (далее BIOS), выдаст ошибку загрузки из-за отсутствия подключения носителей информации. Предложен следующий алгоритм работы комплекса: для идентификации в системе используется (Radio Frequency Identification далее RFID). Ключевым элементом которого является радиометка, которая состоит из:

– чипа – является средством хранения данных;
– антенны – посредством которой передается информация;
– оболочки – защищает антенну и чип от факторов окружающей среды;
– корпуса – также выполняет защитную функцию, но помимо этого еще является и средством крепления к объектам учета.

RFID карта MIFARE Classic представлена на рисунке 1.

Рис. 1. RFID карта MIFARE Classic

Одним из важных элементов системы является считывающее устройство (ридер). Процесс его работы организован следующим образом. Ридер отправляет сигнал чипу, который воспринимает его с помощью антенны и отправляет сигнал-ответ. Считывающее устройство его принимает и обрабатывает для дальнейшего использования в нашей системе. Использование данного способа идентификации – обеспечивает следующие преимущества: метки отличаются высокой безопасностью и сложностью подделки; устойчивостью к незначительным механическим воздействиям и факторам окружающей среды; возможностью хранения не только основных данных, но и дополнительной информации. При поднесении метки к ридеру считывается ключ, в результате обработки которого происходит разблокирование одного из носителей информации после этого пользователь может запустить операционную систему, где пройдёт идентификацию посредством сверки введённого им пароля. Структурная схема аппаратно программного комплекса физического разграничения доступа к ПЭВМ представлена на рисунке 2.

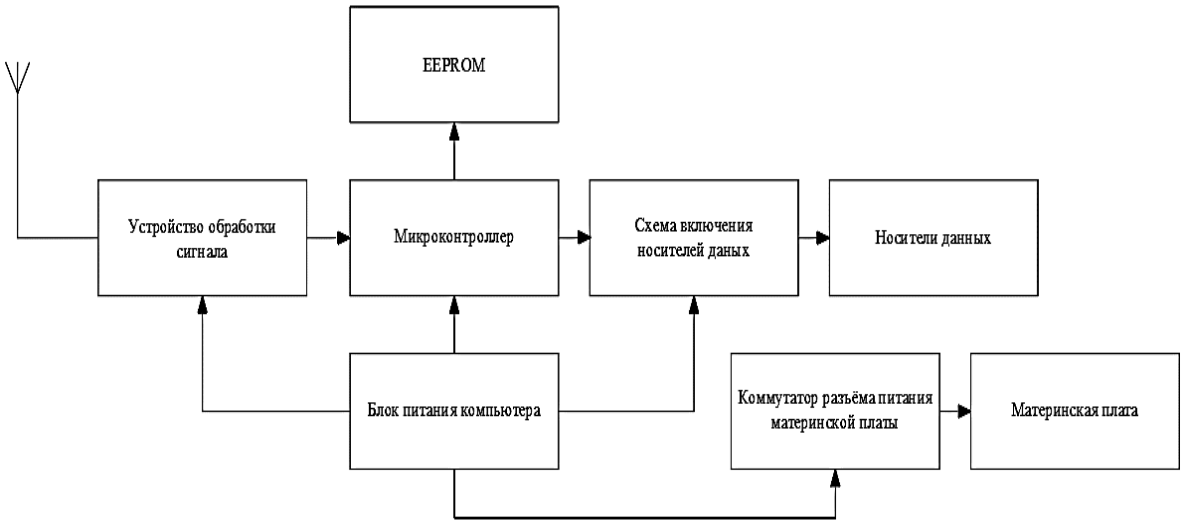

Рис. 2. Структурная схема аппаратно программного комплекса физического разграничения доступа к ПЭВМ

Разработанное устройство рассчитано на 5 носителей информации, электронные ключи хранятся в защищённой от считывания памяти контроллера и могут перезаписываться только при использовании карты с кодом прописанным в самой системе, предоставляемой в комплекте с комплексом. Количество носителей может варьироваться в зависимости от требований заказчика. К достоинствам комплекса можно отнести сравнительно высокую степень защиты благодаря криптозащите карт MIFARE, а так же небольшие габариты и вес что даёт возможность устанавливать в большинство стандартных корпусов ПЭВМ и подключаться к стандартным разъёмам, без создания заметных неудобств в работе пользователя.

По результатам проведённых исследований и лабораторной апробации разработан аппаратно программный комплекс физического разграничения доступа ПЭВМ. Данный комплекс может быть использован в различных организациях для защиты от утечек информации, который можно использовать в большинстве организаций для защиты от утечек информации, благодаря простоте и надёжности которого позволяют конкурировать с аналогичными решениями на программном уровне.

Список использованных источников

1. Рудометов Е. Материнские платы и чипсеты // Питер. 2007. 220 с.
2. Хоровиц П., Хилл У. Искусство схемотехники // М.: 2014. 161 с.
3. Хорев П. Б. Программно-аппаратная защита информации // «Форум». 2019