УДК 004.056.5

ИСПОЛЬЗОВАНИЕ ФИЗИЧЕСКОГО РАГРАНИЧЕНИЯ ДОСТУПА ПЭВМ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ В МЕДИЦИНЕ

МАРМУЗЕВИЧ М.А., БУНЕВИЧ М.А. МАЙОРОВ А.И.

Белорусский государственный университет информатики и радиоэлектроники

(г. Минск, Республика Беларусь)

Аннотация. Один из основных путей решения медицинских, социальных и экономических задач является использование информационных технологий в медицине. Целью данной работы была разработка аппаратно программного комплекса для защиты и ограничения доступа к служебной медицинской 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, применяемых как в медицинских лабораторных исследованиях, так и при обработке данных пациентов.

Ключевые слова: ПЭВМ, физическое разграничение доступа, информационные технологии, медицина, RFID, электронные ключи.

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов

PHYSICAL ACCESS CONTROL FOR PC IN INFORMATION TECHNOLOGY AND MEDICINE

MARMUZEVICH M.A. BUNEVICH M.A. MAYORAU A.I.

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. One of the main ways to solve medical, social and economic problems is the use of information technologies in medicine. The purpose of this work was to develop a hardware and software complex for protecting and restricting access to service medical 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 used both in medical laboratory research and in processing patient data.

Keywords: PC, physical access control, information technologies, medicine, RFID, electronic keys.

Conflict of interests. The authors declare no conflict of interests.

Введение

С каждым годом в медицине повышается уровень автоматизации исследований и объёма обработки массивов информации. Большинство современных медицинских исследований основаны на использовании вычислительной техники. Данные, вводимые в компьютер, формируют базу данных, которая, обрабатывается с помощью специального программного обеспечения. Такая база может содержать, истории болезни, рентгеновские снимки в цифровом виде, статистическую отчетность по стационару, бухгалтерский учет и другую специальную медицинскую информацию. Целью специальных прикладных программ являются вычисления и обработка результатов исследований, расчеты, обмен информацией между компьютерами и посредством сети. Задача разграничения доступа направлена в первую очередь на предотвращение реализации угрозы нарушения конфиденциальности или несанкционированного доступа к информации медицинского назначения. 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.

Один из основных путей решения медицинских, социальных и экономических задач является использование информационных технологий в медицине. С этим связаны задачи поиска действенных инструментов, способных обеспечить повышение основных показателей в области медицины, качества лечения, уровня безопасности пациентов, эффективности медицинской помощи.

В тоже время достаточно сложно организовать контроль за действиями медицинского работника, обрабатывающего конфиденциальными данные пациентов на ПЭВМ [1]. Путём атак на сред-

ства аутентификации для получения пароля или других данных для идентификации, с помощью которых возможно получить доступ к системе или уничтожить важную медицинскую информацию и массивы данных лабораторных исследований.

Целью данной работы была разработка аппаратно программного комплекса, для защиты и ограничения доступа к служебной медицинской информации путём дополнительной идентификации пользователя в системе.

Описание состава комплеса

При включении компьютера, Basic Input/Output System (далее BIOS) выдаст ошибку загрузки из-за отсутствия подключения носителей информации [2]. В статье предложен алгоритм работы комплекса включающий использование: Radio Frequency Identification далее RFID для доступа к носителям информации. Ключевым элементом идентификации является RFID карта, 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.

Строение карты RFID MIFARE Classic представлено на рисунке 1.

Рисунок 1 – Строение RFID карты MIFARE Classic

Разрабатываемая система включает считывающее устройство (ридер). Алгоритм его работы состоит в следующем: считыватель отправляет сигнал чипу, который принимает его с помощью антенны и отправляет сигнал-ответ. Считыватель принимает такой сигнал и конвертирует в цифровой код, для дальнейшего использования в системе. Использование предложенного алгоритма идентификации обеспечивает следующие преимущества: высокий уровень защищенности и сложность копирования информации с RFID карты доступа; устойчивость к механическим воздействиям; возможность хранения дополнительной информации.

Разработка алгоритма работы комплекса и апробация прототипа

При чтении RFID карты ридером считывается информация о цифровом ключе. После обработки полученных данных и их сравнения происходит коммутация соответствующего носителя информации [3]. Пользователь после идентификации запускает операционную систему, и затем начинается следующая ступень идентификации путём ввода личных данных - логина и пароля. Структурная схема предложенного аппаратно программного комплекса физического разграничения доступа к ПЭВМ представленная на рисунке 2.

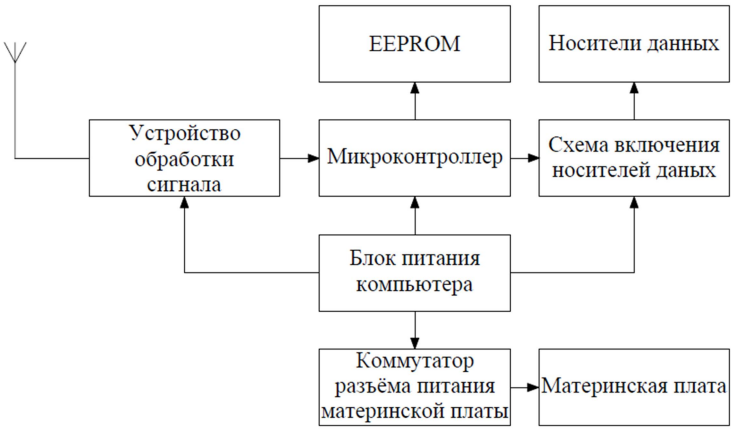


Рисунок 2 – Структурная схема аппаратно программного комплекса физического разграничения доступа к ПЭВМ

Устройство обработки сигнала комплекса состоит из двух основных компонентов: транспондера (метки) расположенного внутри карты и устройства считывания карт (приемопередатчик). Схематичное представление устройства обработки сигналов показано на рисунке 3.

Рисунок 3 – Схематичное представление принципа работы устройства обработки сигналов

Ридер включает в себя радиочастотный модуль, блок управления и антенную катушку. Высокочастотное электромагнитное поле генерируется катушкой. С другой стороны, метка представляет собой пассивный элемент, состоящий из антенны и микросхемы. Поэтому, когда метка вносится в электромагнитное поле устройства считывания карт (приемопередатчик) в его антенне образуется индукционное напряжение, которое запитывает чип карту, затем чип отправляет цифровой код считывателю.

Схематично индукционная связь антенн приёмника и электронной карты представлена на рисунке 4.

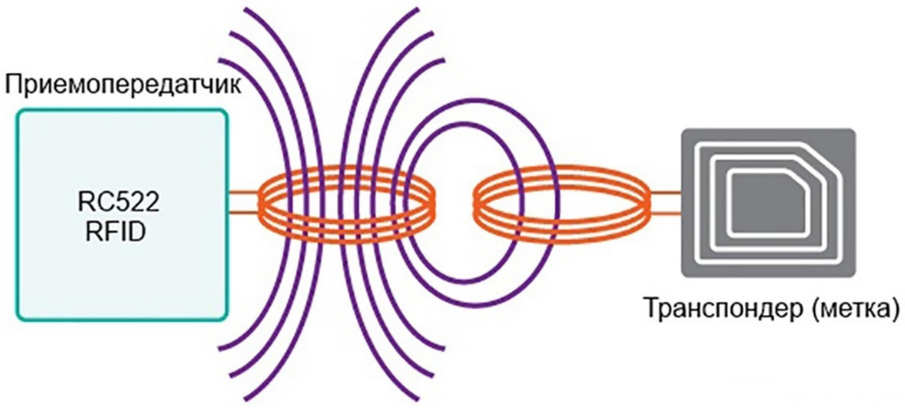
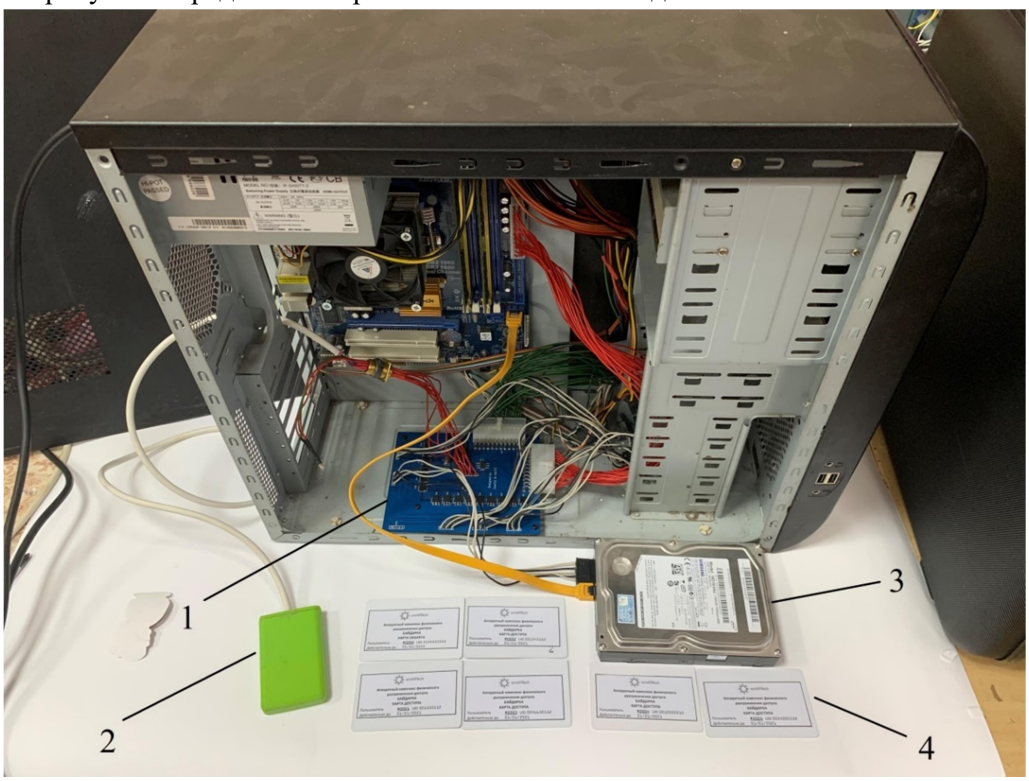


Рисунок 4 – Схематичное представление индукционной связи антенн карты и считывателя.

Модуль RFID RC522 генерирует электромагнитное поля с частотой 13,56 МГц, которое используется для связи с RFID метками (стандартные метки ISO 14443A). Для взаимодействия с контроллерами, модуль использует 4-х контактный интерфейс SPI считывателя.

На рисунке 5 представлен прототип комплекса с подключённым ПЭВМ.



1 – Плата комплекса, 2 – Считыватель карт RFID, 3 – Подключённый жёсткий диск, 4 – Ключ карты MIFARE

Рисунок 5 – Подключение комплекса физического разграничения доступа к ПЭВМ

Комплекс подключён к материнской плате типа ATX, через стандартные разъёмы питания 24pin, коммутация разъёмов жёстких дисков происходит через разъёмы SATA 15pin. Использован полноразмерный корпус типа Midi Tower, с пятью слотами под носители информации.

Заключение

Разработан комплекс, который позволяет подключать до 5 носителей информации: жёстких дисков или твердотельных накопителей. По результатам проведённых исследований предложен алгоритм работы устройства и разработан прототип аппаратно программного комплекса физического разграничения доступа ПЭВМ. Достоинством комплекса является высокая степень защиты, достигаемая с использованием криптозащиты карт MIFARE, а также небольшие массогабаритные характеристики, что позволяет устанавливать комплекс в большинство корпусов ПЭВМ и подключать к стандартным разъёмам. В комплексе обеспечена полная автономность работы, что является важным элементом для компьютеров со слабыми системными характеристиками. Данный комплекс может быть использован в ПЭВМ различных конфигураций, применяемых как в лабораторных медицинских исследованиях, так и при обработке данных пациентов.

Список литературы / References

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

Вклад авторов

Мармузевич М.А.: разработка и отладка аппаратной и программной части комплекса.

Буневич М.А.: постановка задачи, техническое задание.

Майоров А.И.: алгоритм работы

Authors' contribution

Marmuzevich M.A.: development and debugging of the hardware and software of the complex.

Bunevich M.A. : explanation of the problem, technical task.

Mayorau A.I. : working algorithm.

Сведения об авторах

Мармузевич М.А техник НИЧ БГУИР НИЛ 5.3 «Материалы и элементы электронной и сверхпроводниковой техники», студент факультета компьютерного проектирования.

Буневич М.А. младший научный сотрудник НИЧ БГУИР НИЛ 5.3 «Материалы и элементы электронной и сверхпроводниковой техники». Аспирант кафедры ИРТ БГУИР

Майоров А.И. Аспирант кафедры ИРТ БГУИР. Начальник отделения технической защиты информации органов пограничной службы.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6
Белорусский государственный университет информатики и радиоэлектроники
тел. +375-33-304-82-75;
e-mail: marmuzevich@bsuir.by
Мармузевич Михаил Александрович
220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6
Белорусский государственный университет информатики и радиоэлектроники
тел. +375-17-293-89-40;
e-mail: mike_box@bk.ru
Буневич Михаил Алексеевич
220013, Republic of Belarus,
Minsk, P. Brovki str., 6,
Belarusian State University
of Informatics and Radioelectronics
tel. +375-17-293-89-40
e-mail: mail.may2991@gmail.com
Mayorau Andrey

Information about the authors

Marmuzevich M.A. technician SRD of BSUIR Research Laboratory 5.3 "Materials and elements of electronic and superconducting technology.", faculty of computer-aided design student .

Bunevich M.A. Junior Researcher, SRD of BSUIR Research Laboratory 5.3 "Materials and elements of electronic and superconducting technology." PhD student of the BSUIR department IRT.

Mayorov A.I. Head of the department for technical security of information of the border service. PhD student of the BSUIR department IRT.

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki str., 6,
Belarusian State University
of Informatics and Radioelectronics
tel. +375-17-293-89-40
e-mail: marmuzevich@bsuir.by
Marmuzevich Mikhail Aliaksandrovich
220013, Republic of Belarus,
Minsk, P. Brovki str., 6,
Belarusian State University
of Informatics and Radioelectronics
tel. +375-17-293-89-40
e-mail: mike_box@bk.ru
Bunevich Mikhail
220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6
Белорусский государственный университет информатики и радиоэлектроники
тел. +375-17-293-89-40;
e-mail: mail.may2991@gmail.com
Майоров Андрей Игоревич