УДК 629.78:004.08

МОДУЛЬ ХРАНЕНИЯ ИНФОРМАЦИИ: СОВМЕЩЕНИЕ ФУНКЦИЙ САНКЦИОНИРОВАНИЯ ДОСТУПА И ПЕРЕНОСА ИНФОРМАЦИИ В СОСТАВЕ АППАРАТУРЫ СИСТЕМ УПРАВЛЕНИЯ

© 2013 Д. А. Ханевский, Н. В. Соловьёва, А. С. Ананьин, И. Н. Щепочкин

ФГУП НПО автоматики им. академика Н.А. Семихатова, г. Екатеринбург

Рассматривается модуль хранения информации, предназначенный для универсальной, не привязанной к конкретному заказу, реализации функций санкционирования доступа, хранения и переноса информации в составе аппаратуры систем управления.

Модуль хранения информации, санкционирование доступа, аппаратура системы управления, беспроводной канал.

Предпосылки разработки МХИ

Обеспечение определённого уровня доступа – одна из приоритетных задач пускопроверочной аппаратуры. Ко всем перспективным разработкам пускопроверочной аппаратуры систем управления (СУ) предъявляются требования защиты от несанкционированных операций (исключение ошибочных действий по управлению пуском; защита обрабатываемой, хранимой и передаваемой по каналам связи информации от несанкционированного доступа и другие). На сегодняшний день в пускопроверочной аппаратуре НПОА для ракетно-космической тематики (РКТ) задачу санкционирования доступа выполняет набор механических ключей (рис. 1).

СУ РН, как и любая современная цифровая вычислительная система (ЦВС), нуждается в устройстве, позволяющем загружать и выгружать из неё данные различного назначения. Программное обеспечение (ПО) и числовой материал для ввода в пускопроверочную аппаратуру поставляются на оптических носителях информации. По опыту использования оптические носители информации имеют низкие показатели надёжности и требуют особых условий эксплуатации.

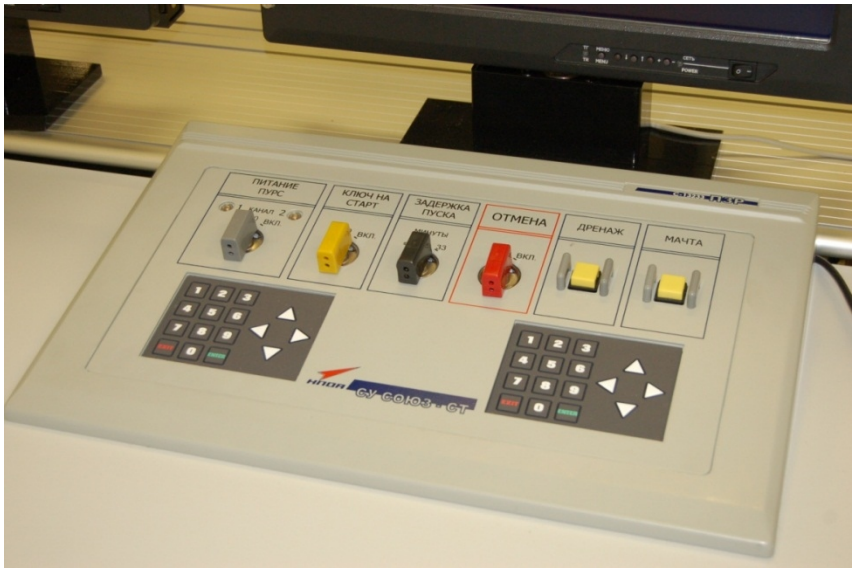

Рис. 1. Набор механических ключей санкционирования доступа в пускопроверочной аппаратуре НПОА для РКТ

Кроме того, жизненный цикл аппаратуры СУ РКТ более 10 лет, но на сегодня отсутствуют покупные приводы, работающие с компактными оптическими дисками и USB Flash, обладающие таким длительным жизненным циклом.

Альтернативным вариантом решения обозначенных проблем и является разрабатываемый в настоящее время в НПОА собственный модуль хранения информации (МХИ). МХИ позволяет решать задачи ввода ПО и числового материала в СУ и вывода диагностической информации из СУ, санкционирования доступа к различного рода операциям: заданию режимов работы, особо ответственным операциям, технологическим операциям. МХИ имеет длительный жизненный цикл эксплуатации (более 10 лет) и будет поставляться за военной приёмкой.

Особенности реализации МХИ и модуля связи МХИ

В состав МХИ входят: вычислительная система на базе микроконтроллера; ПЗУ flash типа; устройство, обеспечивающее питание МХИ и передачу данных по беспроводной линии связи (БЛС) при взаимодействии с модулем связи МХИ (МС МХИ).

Такая структура МХИ позволяет реализовать функцию хранения и передачи данных, а также функцию предоставления доступа к различным операциям с СУ путём хранения числовых ключей в памяти МХИ, а беспроводной канал передачи данных и питания обеспечивает высокий уровень надёжности разрабатываемого прибора.

Структура и внешние связи МХИ показаны на рис. 2.

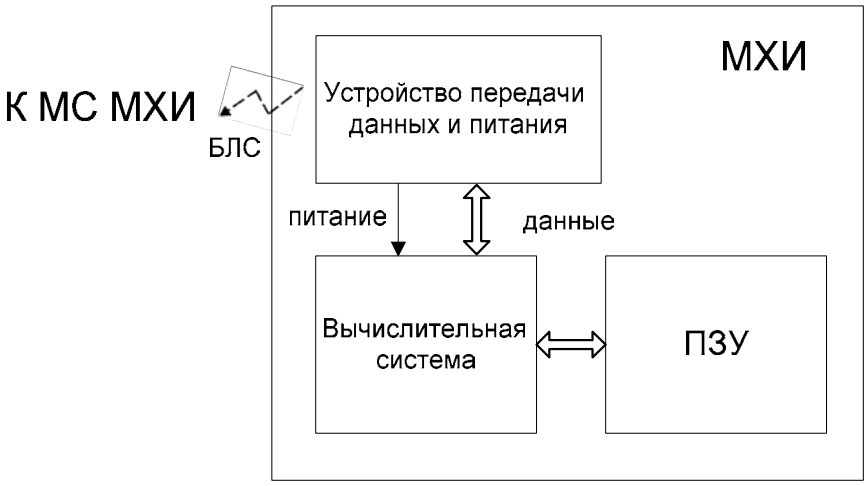

Рис. 2. Структура и внешние связи МХИ

На рис. 3 представлены структура и внешние связи МС МХИ.

Основными элементами МС МХИ являются слот для установки МХИ и устройство передачи данных и питания.

МС МХИ должен обеспечивать передачу данных между ЭВМ верхнего уровня и МХИ. Существует два варианта ЭВМ верхнего уровня, с которыми предусмотрено взаимодействие МХИ:

1. ПЭВМ для работы с МХИ, с которой на МХИ записывается различная служебная информация и комплекты ПО. Таким образом, при помощи ПЭВМ проводится подготовка МХИ к штатной эксплуатации.

2. В штатной эксплуатации – это цифровая вычислительная машина пускопроверочной аппаратуры.

При этом МС МХИ обменивается с ЭВМ верхнего уровня по интерфейсу RS-422, а связь МС собственно с МХИ осуществляется по беспроводной линии связи.

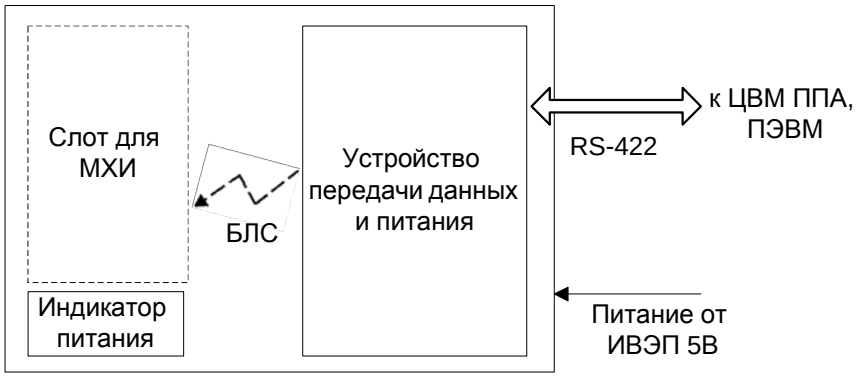

Рис. 3. Структура и внешние связи МС МХИ

Как было отмечено ранее, помимо обеспечения функций хранения и переноса информации МХИ используется как ключ, обеспечивающий доступ оператору к различным операциям с СУ. Возможно создание нескольких типов ключей, обеспечивающих разный уровень доступа к СУ. Типы МХИ, например, могут быть следующими:

- ключ оператора, разрешающий включение питания и базовые операции типа проверочных режимов;
- ключ командира, разрешающий пуск или иные специальные операции (может быть 2-3 ключа командиров, каждый из которых санкционирует свои операции);
- ключ разработчика, открывающий доступ к настройкам системы, например, к установке ПМО.

Отличительными особенностями МХИ являются:

- уникальный для каждого типа МХИ цвет, соответствующий типу МХИ;
- нанесённый на корпус номер, соответствующий типу МХИ;
- нанесённый на корпус МХИ уникальный номер, который присваивается каждому МХИ на этапе изготовления.

Тип и номер каждого ключа можно определить как визуально, так и программно средствами штатного ПО СУ.

Особенности взаимодействия МХИ с ЭВМ верхнего уровня

Как отмечалось ранее, в составе МХИ должна быть Flash-память с возможностью записи и чтения пользовательских данных. При этом Flash-память МХИ разбита на виртуальные страницы (ВС). ВС – это массив данных, который идентифицируется определённым номером. Собственно взаимодействие с МХИ производится путём чтения/записи ВС.

Взаимодействие ЭВМ верхнего уровня с МХИ производится по принципу «запрос – ответ». МХИ является оконечным устройством (ОУ) и должен только отвечать на запросы. Инициатором обмена всегда является ЭВМ верхнего уровня (ПЭВМ или ЦВМ пускопроверочной аппаратуры), функционирующая в режиме контроллера линии (КЛ).

Существуют следующие основные варианты взаимодействия с МХИ: запись виртуальной страницы, считывание виртуальной страницы, стирание памяти МХИ, запрос служебной информации (версия ПО МХИ, скорость обмена и др.), работа с шифрованием (запись закрытого ключа, запрос на шифрование сообщения).

Рассмотрим, каким образом обеспечивается аутентификация МХИ при его установке в пультовую аппаратуру и как обеспечивается защита информации, передаваемой от МХИ к управляющей ЦВМ.

Защиту информации, циркулирующей в канале связи ЦВМ с МС МХИ, предлагается обеспечивать посредством асимметричного шифрования данных на математическом аппарате эллиптических кривых с применением отечественного алгоритма ГОСТ Р 34.10-2001 [1]. Использование симметричных алгоритмов шифрования для санкционирования доступа неудобно необходимостью решать проблемы хранения и/или передачи закрытых ключей по открытым каналам связи. Асимметричные криптосхемы лишены этих недостатков [2].

Санкционирование производится путём обмена шифрованными сообщениями между ЦВМ, принимающей решения о санкции, и МХИ. При этом информация для санкционирования доступа на всём пути следования остается зашифрованной, что снимает требования по защите трактов передачи от прослушивания или иного вмешательства.

Управляющая ЦВМ должна иметь в памяти набор открытых ключей, каждый из которых должен соответствовать заводскому номеру МХИ. Управляющая ЦВМ отправляет в МХИ пакет, содержащий сообщение для шифрования, а МХИ зашифровывает полученное сообщение на своём закрытом ключе и отправляет обратно в качестве ответного пакета. ЦВМ, получив зашифрованное сообщение, дешифрует его и сравнивает с отправленным сообщением. Сообщение для шифрования - это псевдослучайное сгенерированное число, при этом для каждого сеанса проверки аутентичности МХИ число должно быть различным. Алгоритм генерации псевдослучайных чисел определяется разработчиком ПО управляющей ЦВМ. Таким способом проводится аутентификация МХИ при его установке в пультовую аппаратуру.

Следует отметить, что область памяти МХИ, предназначенная для записи закрытого ключа и параметров шифрования, недоступна для чтения в штатном режиме работы. Служебную информацию можно изменить только на АРМ МХИ. В остальных случаях она доступна только для чтения.

Перспективы внедрения МХИ в РКТ

Пультовая аппаратура формирует имидж разработчика и производителя. От того, как выглядит пульт управления и как он функционирует, зависит впечатление от работы комплекса в целом.

Универсальным, не привязанным к конкретному заказу, позволяющим эффективно осуществлять функции санкционирования доступа решением является внедрение МХИ совместно с применением сенсорной клавиатуры (рис. 4).

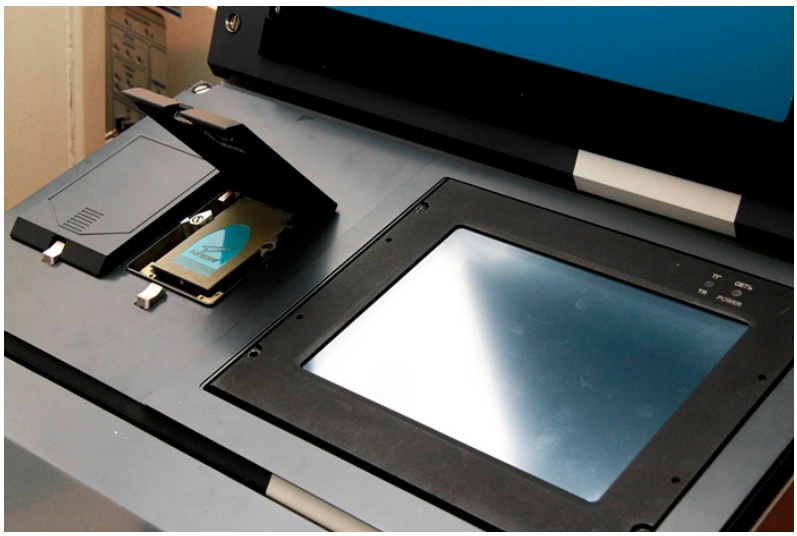

Рис. 4. Перспективный вариант совместного внедрения МХИ и сенсорной панели в пультовую аппаратуру СУ

В данном случае МХИ санкционирует доступ к определённым операциям, а особенности конкретного заказа учитываются через ПМО (путём обработки информации, вводимой с сенсорной клавиатуры). Внедрение МХИ совместно с применением сенсорной клавиатуры позволит полностью исключить механические элементы из пультовой аппаратуры СУ.

Библиографический список

1. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Текст] / – М.: Госстандарт России, 2001.

2. Романец, Ю. В. Защита информации в компьютерных системах и сетях [Текст] / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин; под общ. ред. В. Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.

MODULE OF STORING INFORMATION: COMBINING THE FUNCTIONS OF AUTHORIZING ACCESS AND TRANSFER OF INFORMATION WITHIN THE CONTROL SYSTEM EQUIPMENT

© 2013 D. A. Hanevsky, N. V. Solovieva, A. S. Ananyin, I. N. Shchepochkin

Federal State Unitary Enterprise Scientific and Production Association of Automation named after academician N.A.Semikhatov, Yekaterinburg

The paper presents a module of information storage, designed for universal, not connected with a particular order, realization of the functions of authorizing access, storage and transfer of information within the equipment of a control system.

Module of information storage, access authorization, equipment of control system, wireless channel.

Информация об авторах

Ханевский Дмитрий Алексеевич, начальник отдела, ФГУП «НПО автоматики имени академика Н.А. Семихатова», г. Екатеринбург. E-mail: artrax@e1.ru. Область научных интересов: структурное проектирование аппаратуры СУ, системотехника, операционные системы реального времени.

Соловьёва Наталья Владимировна, кандидат технических наук, доцент, заместитель начальника отдела, ФГУП «НПО автоматики имени академика Н.А. Семихатова», г. Екатеринбург. E-mail: soloveva-nv@mail.ru. Область научных интересов: структурное проектирование аппаратуры СУ, защита информации в управляющих системах.

Ананьин Александр Сергеевич, инженер-конструктор, ФГУП «НПО автоматики имени академика Н.А. Семихатова», г. Екатеринбург. E-mail: am2per@gmail.com. Область научных интересов: системотехника, структурное проектирование аппаратуры СУ.

Щепочкин Игорь Николаевич, начальник группы, ФГУП «НПО автоматики имени академика Н.А. Семихатова», г. Екатеринбург. E-mail: igor.shepochkin@mail.ru. Область научных интересов: алгоритмы и устройства помехозащищённого обмена информацией, математическое моделирование, криптография.

Hanevsky Dmitri Alexeyevich, head of department, Scientific and Production Association of Automation. E-mail: artrax@e1.ru. Area of research: structured design of control systems, system engineering, real time operating systems.

Solovieva Natalya Vladimirovna candidate of engineering, associate professor, deputy head of department, Scientific and Production Association of Automation. E-mail: soloveva-nv@mail.ru. Area of research: structured design of control systems, information security in control systems.

Ananyin Aleksandr Sergeevich design engineer, Scientific and Production Association of Automation. E-mail: am2per@gmail.com. Area of research: structured design of control systems, system engineering.

Shchepochkin Igor Nikolayevich, team chief, Scientific and Production Association of Automation. E-mail: igor.shepochkin@mail.ru. Area of research: algorithms and devices of noise immunity in information exchange, mathematical modeling, cryptography.