МОДУЛЬ ДОВЕРЕННОЙ ЗАГРУЗКИ С ВОЗМОЖНОСТЬЮ УДАЛЕННОГО УПРАВЛЕНИЯ СЕРВЕРАМИ

TRUSTED BOOT MODULE WITH THE ABILITY OF REMOTE MANAGING OF SERVERS

УДК 004.056

РОМАНЕЦ ЮРИЙ ВАСИЛЬЕВИЧ

ДУДАРЕВ ДМИТРИЙ АЛЕКСАНДРОВИЧ

ПАНАСЕНКО СЕРГЕЙ ПЕТРОВИЧ

ООО Фирма «АНКАД»
124527, г. Москва, г. Зеленоград, Солнечная аллея, 8
integration@ancud.ru

ROMANETS YURY V.

DUDAREV DMITRY A.

PANASENKO SERGEY P.

"ANCUD" Ltd.
8 Solnechnaya Alley, Zelenograd, Moscow, 124527, Russia
integration@ancud.ru

Аппаратно-программные модули доверенной загрузки позволяют обеспечить контроль и разграничение доступа к ресурсам компьютера на основе строгой двухфакторной аутентификации, а также контроль целостности используемой программной среды. Их оснащение функциями управления серверами позволяет обеспечить надежное и безопасное управление серверами в клиент-серверных архитектурах.

Ключевые слова: удаленное управление; контроль доступа; аутентификация; АПМДЗ; защита данных.

Trusted boot modules make it possible to control and manage access to computers and their resources as well as to control the integrity of the installed software environment. They are usually based on mechanisms of strong two-factor authentication. Equipping trusted boot modules with server management features allows providing reliable and secure management of servers in client-server architectures.

Keywords: remote control; access restriction; authentication; trusted boot modules; information protection.

В настоящее время разработан ряд технологий, являющихся стандартами в области встроенных систем управления и обслуживания серверов, которые базируются на использовании интеллектуального интерфейса управления платформой (IPMI — Intelligent Platform Management Interface), предназначенного для мониторинга и управления сервером. Спецификация IPMI была разработана в 1998 г. корпорацией Intel и используется многими ведущими производителями компьютеров [1].

Интерфейс IPMI предназначен для автономного мониторинга и управления функциями, встроенными непосредственно в аппаратное и микропрограммное обеспечение серверных платформ. Данный интерфейс имеет, в частности, следующие возможности удаленного управления и мониторинга:

- мониторинг ряда технических параметров сервера, включая температуру основных аппаратных блоков, напряжение и состояние источников питания, скорость вращения вентиляторов, наличие ошибок на системных шинах и др.;
- включение/выключение и перезагрузка компьютера;
- определение выходящих за пределы допустимых диапазонов и аномальных состояний и их фиксация для последующего исследования и предотвращения;
- ряд других функций по управлению сервером.

Аппаратной составляющей IPMI является встроенный в платформу автономный контроллер, который носит название BMC (Baseboard Management Controller — контроллер управления материнской платой) и работает независимо от центрального процессора, базовой системы ввода-вывода (BIOS — Basic Input/Output System) и операционной системы (ОС) компьютера, обеспечивая управление серверной платформой даже в тех случаях, когда сервер выключен (достаточно лишь подключения к источнику питания). Контроллер BMC имеет собственный процессор, память и сетевой интерфейс.

Подробное описание структуры и принципа функционирования IPMI, а также функций контроллера BMC на сервере, обеспечивающих контроль его состояния и управление, приведены, в частности, в работе [2].

Практика показывает, что использование для критичных информационных технологий зарубежной компьютерной техники, комплектующих и программного обеспечения (ПО), производители которых не дают полной информации о своей продукции, не гарантирует отсутствия в ней недекларируемых возможностей, следовательно, не позволяет гарантировать требуемую степень защиты от несанкционированного доступа (НСД) к критичным компонентам информационно-вычислительных систем (ИВС) и их информационным ресурсам.

Это может усугубляться недостаточно проработанными механизмами защиты; в частности, в IPMI-системах удаленного доступа проводится однофакторная аутентификация по паролю, в то время как при использовании отечественных устройств создания доверенной среды — аппаратно-программных модулей доверенной загрузки (АПМДЗ) при доступе к ИВС и ее компонентам применяется двухфакторная аутентификация, при которой, помимо пароля, требуется предъявить специальный аутентифицирующий носитель пользователя (АНП). Кроме того,

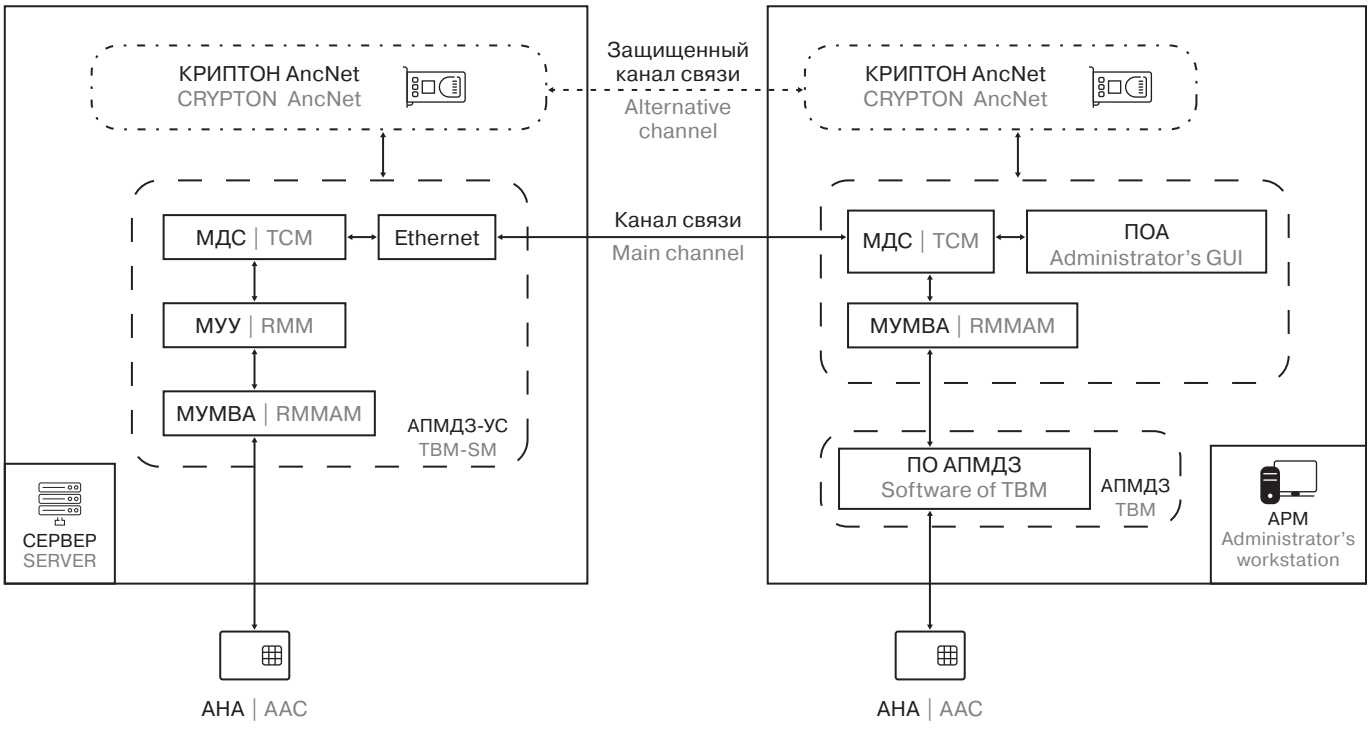

Рис. 1. Схема системы удаленного управления сервером
Fig. 1. The structure of the server remote management system

в компьютерных системах на базе АПМДЗ создается доверенная среда за счет интеграции с данным модулем различных средств защиты информации, включая криптографические средства, в комплексную систему защиты ИВС.

В связи с тем, что интерфейс IPMI, с одной стороны, дает масштабные возможности по управлению сервером, а с другой стороны, использует слабую однофакторную аутентификацию по паролю, можно утверждать, что данный интерфейс представляет потенциальную опасность атак на сервер (в т. ч. выключенный) через Интернет, увеличивая вероятность несанкционированного доступа к его ресурсам.

Отметим также, что некоторые из экспертов по информационной безопасности обращают внимание на тот факт, что с помощью контроллера BMC через интерфейс IPMI можно удаленно полностью контролировать аппаратное и программное обеспечение серверов. Это дает злоумышленнику практически

INTRODUCTION

Several technologies have recently been developed, which are standards in the field of embedded server management and maintenance systems. Some of them are based on the use of IPMI — Intelligent Platform Management Interface, designed for server monitoring and management. The IPMI specification was developed in 1998 by Intel Corporation and is used by many leading computer manufacturers [1].

The IPMI interface is designed for remote monitoring and management of functions built directly into the hardware and firmware of server platforms. This interface has, in particular, the following remote control and monitoring capabilities:

- monitoring of some of technical parameters of the server, including the temperature of the main hardware units, voltage and status of power supplies, fan speed, the presence of errors on system buses etc.;
- switching on/off and restarting the computer;
- detection of out-of-range and anomalous states and their fixing for further investigation and prevention;
- a number of other functions to manage the server.

The hardware component of IPMI is a standalone controller built into the platform called BMC. It operates independently of the CPU, the basic input/output system (BIOS) and the operating system of the computer. BMC provides the server platform management, even when the server is turned off (just connected to the power supply). The controller has its own processor, memory and network interface.

The detailed description of the structure and functioning of IPMI, as well as the functions of the BMC controller on the server (providing control and monitoring of its state), are given, in particular, in the paper [2].

The experience has shown that the use of untrusted computer hardware and software components for critical information technologies, whose manufacturers do not give full information about their products, does not guarantee the absence of their undeclared capabilities. Therefore it does not make it possible to guarantee the required degree of protection against unauthorized access to the critical components of computer systems and their information resources.

This may be exacerbated by the use of inappropriate protection mechanisms. In particular, one-factor password authentication is usually performed in remote access systems based on IPMI. It is in contrast to trusted boot modules, which in general use two-factor authentication: in addition to the password, they require inserting a special authenticating user carrier. Besides, trusted boot modules allow creating a trusted environment in computer systems by integrating

неограниченные возможности по несанкционированному воздействию на них в случае получения контроля над IPMI (см., например, [3–5]).

Данный факт подтверждает обоснованность требований отечественного регулятора в дополнительной защите серверов и автоматизированных рабочих мест (АРМ) ИВС с помощью АПМДЗ.

АПМДЗ предназначены для обеспечения контроля и разграничения доступа пользователей к компьютерам и его аппаратным ресурсам, контроля целостности установленной на компьютере программной среды, а также для выполнения ряда других защитных функций.

Примером АПМДЗ является разработанное ООО Фирма «АНКАД» семейство устройств «КРИПТОН-ЗАМОК». Данные устройства имеют следующие основные возможности:

- идентификация и усиленная аутентификация пользователей до загрузки ОС компьютера;
- аппаратная защита от загрузки ОС со сменных носителей;
- контроль целостности программной среды;
- разграничение доступа к ресурсам компьютера;
- создание нескольких контуров защиты;
- удаленное централизованное управление и администрирование;
- работа с различными ключевыми носителями;
- безопасное хранение собственного доверенного ПО на встроенной флэш-памяти;
- возможность интеграции с различными аппаратными и программными средствами защиты информации.

АПМДЗ данного семейства могут быть выполнены как в виде платы расширения, подключаемой к материнской плате компьютера [6], так и в виде набора микросхем, интегрированного непосредственно в материнскую плату [7].

Оснащение АПМДЗ семейства «КРИПТОН-ЗАМОК» рядом дополнительных аппаратных компонентов и программных модулей, обеспечивающих выполнение функций удаленного управления серверами, позволяет обеспечить безопасное выполнение ряда функций по удаленному управлению, свойственных контроллеру BMC.

На основе такого варианта АПМДЗ может быть разработана система, в которую, на верхнем уровне, входят следующие два компонента (см. рис. 1):

- управляемый сервер, оснащенный устройством «КРИПТОН-ЗАМОК», включающим компоненты и модули удаленного управления серверами;
- АРМ администратора, оснащенный классическим АПМДЗ семейства «КРИПТОН-ЗАМОК», но с установленными на уровне ОС программными модулями, взаимодействующими с модулями установленного на управляемый сервер устройства «КРИПТОН-ЗАМОК» и совместно с ними обеспечивающими строгую удаленную аутентификацию администраторов и удаленное управление сервером.

Опишем основные принципы функционирования предложенной системы удаленного управления сервером.

На подготовительном этапе работы системы выполняются действия по ее установке и настройке, которые сводятся к следующим операциям:

1. На управляемый сервер устанавливается устройство АПМДЗ с функциями удаленного управления серверами (АПМДЗ-УС), включающее в себя (помимо обычного набора модулей базового АПМДЗ «КРИПТОН-ЗАМОК») следующие программные модули:
   - модуль доверенного соединения (МДС);
   - модуль удаленной многофакторной взаимной аутентификации (МУМВА);
   - модуль удаленного управления (МУУ); модули МУМВА и МУУ выполняются в доверенной среде АПМДЗ-УС.
2. На АРМ администратора устанавливается классическое устройство АПМДЗ, в качестве которого, в частности, может использоваться одно из устройств семейства «КРИПТОН-ЗАМОК» (см., например, [6, 7]).

with the module various information security tools (including cryptographic hardware or software), into a comprehensive IT protection system.

Due to the fact that the IPMI interface, on the one hand, provides large-scale server management capabilities, and on the other, it uses weak one-factor authentication by password, it can be argued that this interface represents a potential danger of attacks on the server (including switched off) via the Internet, increasing the likelihood of unauthorized access to its resources.

We can also note that some of the information security experts pay attention to the fact that with the help of the BMC controller through the IPMI interface it is possible to control the servers hardware and software remotely. This gives the attacker almost unlimited opportunities for their unauthorized exposure in the event of gaining control over IPMI (see, for example, [3–5]).

This fact confirms the validity of the requirements for providing an additional protection of servers and workstations based on the use of trusted boot modules (TBM).

DESCRIPTION

The main goals of trusted boot modules are to control and delimitate users' access to computers and their hardware resources, to control the integrity of the software environment installed on the computer, and to perform a number of other protective functions.

Let us consider Crypton-Zamok devices by ANCUD Ltd. as an example of trusted boot modules. Crypton-Zamok is the series of devices that provide the following basic possibilities:

- user identification and strong authentication before starting the computer operating system load;
- the hardware protection against loading OS from removable media;
- controlling the integrity of the software environment;
- delimitation of access to computer resources;
- creating several protection contours;
- remote and centralized management and administration;
- the ability to use different types of key carriers;
- secure storage of their own trusted software and firmware in built-in flash memory;
- the possibility of integrating with various information protection hardware and software.

Trusted boot modules of this series can be realized both in the form of an expansion board connected to the motherboard of the computer [6] and as a set of microchips integrated directly into the motherboard [7].

Equipping the trusted boot modules of this series with a set of additional hardware

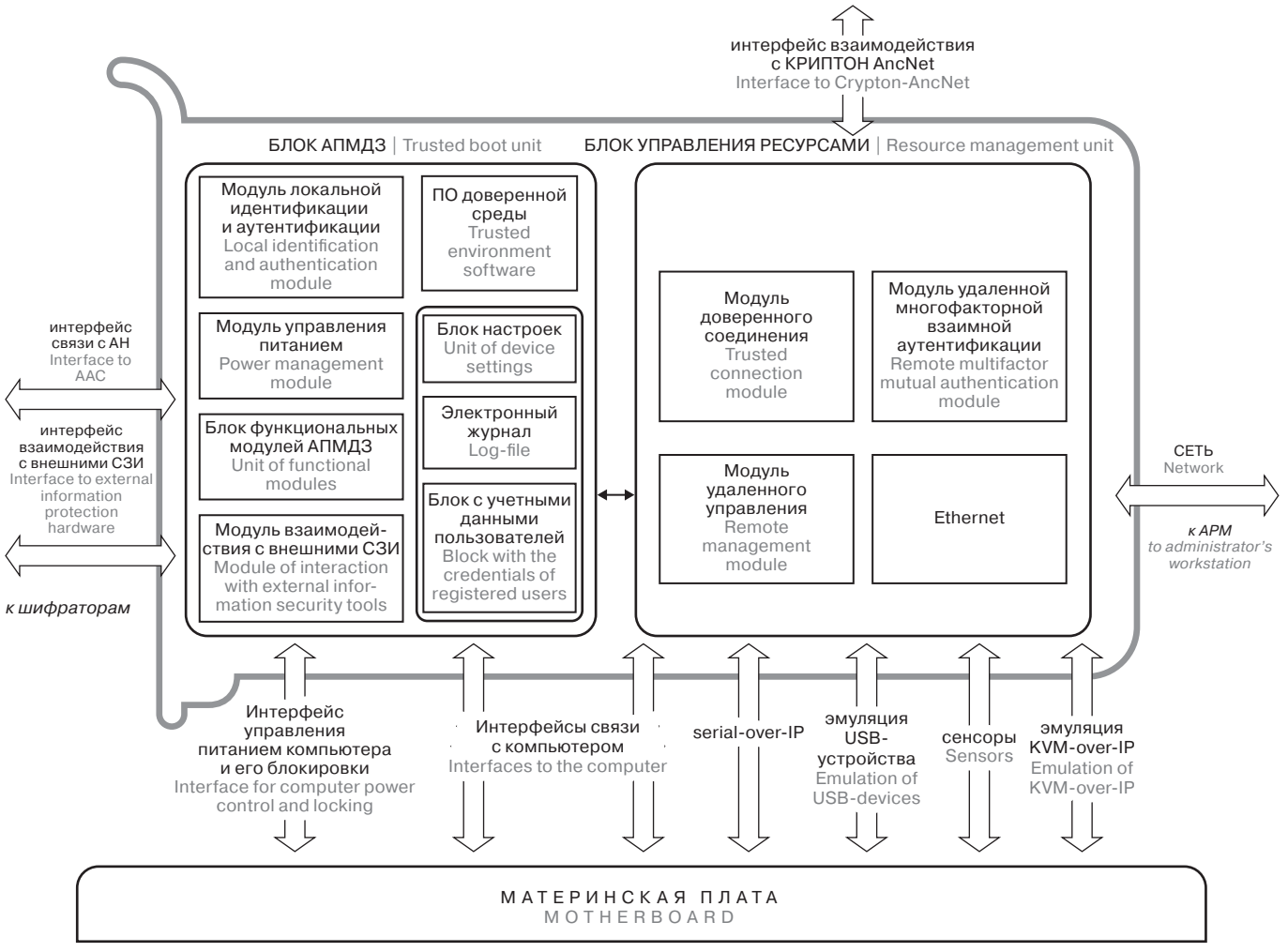

Рис. 2. Схема устройства АПМДЗ-УС
Fig. 2. The structure of the TBM-SM device

components and software modules providing remote server management functions allows the secure execution of remote management functions specific to the BMC.

Therefore, it is possible to develop a protected system based on this kind of trusted boot modules. At the top level the system includes the following two components (Fig. 1):

- a managed server equipped with Crypton-Zamok device that includes components and modules for remote server management;
- an administrator's workstation equipped with a classic Crypton-Zamok device as well as specific software modules installed on the OS level that interact with the modules of the Crypton-Zamok device, installed on the managed server, and jointly provide strict remote authentication of the administrator and remote server management.

Let us describe the basic principles of functioning of the proposed remote server management system.

At the preliminary stage, the installation and configuration actions are performed, which include the following operations:

1. The managed server is equipped with a trusted boot module with the functions of remote server management (TBM-SM); in addition to the usual set of modules of the base Crypton-Zamok device, it includes the following software modules:
   - trusted connection module (TCM);
   - remote multifactor mutual authentication module (RMMAM);
   - remote management module (RMM);

   the RMMAM and RMM modules are executed in the trusted environment of the TBM-SM.
2. A classic trusted boot module is installed on the administrator's workstation; one of the set of Crypton-Zamok devices can be used here (see, for example, [6, 7]).
3. The specific software modules are installed on the administrator's workstation to provide the mutual authentication between the managed server and workstations, a secure communication channel between them and remote management of the server. These modules include RMMAM, TCM and administrator's graphical user interface (GUI).

The trusted boot module installed on the administrator's workstation performs the strict user authentication on the workstation and its trusted loading. This TBM is also used to check the integrity of the software components loaded to the workstation, including the RMMAM, TCM and administrator's GUI.

In addition, the trusted boot module on the administrator's workstation can be used to store the above-mentioned modules (the RMMAM, TCM and administrator's GUI)

3. На АРМ администратора загружаются программные модули, обеспечивающие взаимную аутентификацию управляемого сервера и АРМ, защищенный канал связи между ними и удаленное управление сервером: МУМВА, МДС и программное обеспечение администратора (ПОА).

Устанавливаемый на АРМ администратора АПМДЗ осуществляет строгую аутентификацию пользователя на АРМ и его доверенную загрузку. Данный АПМДЗ также используется для контроля целостности программных компонентов АРМ, в частности, загружаемых на АРМ программных модулей МУМВА, МДС и ПОА.

Кроме того, АПМДЗ на АРМ администратора может использоваться для хранения перечисленных выше модулей МУМВС, МДС и ПОА в собственной энергонезависимой памяти и их загрузки в целевую операционную систему АРМ администратора.

В штатном режиме работы система удаленного управления сервером обеспечивает выполнение следующей последовательности действий:

1. Выполняется двухфакторная взаимная аутентификация администратора на основе данных, считываемых с аутентифицирующего носителя администратора (АНА) на АРМ администратора, и данных, сохраненных на сервере во время регистрации администратора на предварительном этапе; аутентификация производится с помощью работающих на сервере и АРМ программных модулей МУМВА на основе данных, полученных в рамках предварительного выполнения локальной аутентификации администратора с помощью АПМДЗ АРМ администратора.
2. Модулями доверенного соединения на стороне сервера и АРМ администратора формируется защищенный канал связи между сервером и АРМ администратора; данный защищенный канал организуется на базе технологии виртуальных частных сетей (VPN — Virtual Private Network), что позволяет инкапсулировать в защищенный канал трафик различных протоколов, включая используемые в рамках взаимодействия по интерфейсу IPMI.
3. С помощью модуля МУУ организуется передача управляющей информации между АРМ администратора и управляемым сервером.
4. Процесс администрирования сервера осуществляется с помощью ПОА, работающего в операционной системе АРМ администратора.

При необходимости управляемый сервер и АРМ администратора могут быть опционально оснащены устройствами «КРИПТОН AncNet» [8]. Данное устройство представляет собой криптографический сетевой адаптер, выполняющий проходное шифрование передаваемых через него данных. С помощью устройств «КРИПТОН AncNet» может быть создан альтернативный, криптографически защищенный канал для передачи данных между сервером и АРМ администратора.

Для выполнения целого ряда дополнительных функций, обеспечивающих удаленное управление серверами, устройство АПМДЗ-УС претерпело значительные изменения по сравнению с базовым АПМДЗ. Схема устройства АПМДЗ-УС приведена на рис. 2.

Устройство состоит из двух основных функциональных блоков, находящихся на общей плате:

- блока АПМДЗ, логически объединяющего основные функции, присущие аппаратно-программным модулям доверенной загрузки;
- блока управления ресурсами, включающего в себя дополнительные функции, включая функции удаленного управления серверами.

Блок АПМДЗ включает в себя следующие компоненты:

- модуль локальной идентификации и аутентификации, осуществляющий локальную аутентификацию пользователей и доверенную загрузку компьютера;
- модуль управления питанием, реализующий, независимо от чипсета материнской платы компьютера, управление основным питанием компьютера и блокировку компьютера в случае обнаружения системой защиты нарушений;

in its own nonvolatile memory and to load them into the target operating system of the administrator's workstation.

In the regular mode of operation, the remote server management system provides the following sequence of actions:

1. Two-factor mutual authentication of the administrator is performed. It is based both on the data read from the administrator's authenticating carrier (AAC) on the administrator's workstation and the data stored on the server during the registration of the administrator in the preliminary stage. The authentication is performed using the RMMAM software modules running on the server and on the administrator's workstation. As mentioned above, it uses the data obtained during the administrator local authentication performed by the trusted boot module installed on the administrator's workstation.
2. The TCM modules (on the server side and on the administrator's workstation) provide a secure communication channel between the server and the administrator's workstation. This protected channel is organized on the basis of Virtual Private Network (VPN) technology, which allows encapsulating the traffic of various protocols into the protected channel, including those used during the interaction via the IPMI interface.
3. The remote management modules on both sides allow transferring the control information between the administrator's workstation and the managed server.
4. The functions of server administration can be carried out with the use of the administrator's GUI, operating in the system of the administrator's workstation.

If required, the managed server and the administrator's workstation can be optionally equipped with Crypton-AncNet devices. This device is a cryptographic network adapter that performs pass-through encryption of data transmitted through it. Using Crypton-AncNet devices, an alternative cryptographically protected channel can be created to transfer data between the server and the administrator's workstation.

The TBM-SM device has undergone significant changes in comparison with the base trusted boot module to perform a set of additional functions that provide remote management of servers. The scheme of the TBM-SM device is shown on Fig. 2.

The device consists of two main function blocks on a common board:

- trusted boot unit that logically combines the basic functions usually inherent in the trusted boot modules;
- resource management unit that integrates additional functions, including remote server management functions.

- блок функциональных модулей, выполняющих штатные функции АПМДЗ;
- модуль взаимодействия с внешними (по отношению к устройству АПМДЗ-УС) средствами защиты информации (СЗИ);
- программное обеспечение доверенной среды;
- блок настроек устройства АПМДЗ-УС, содержащий список контролируемых аппаратных и программных объектов, настройки и ключи централизованного администрирования, а также дополнительные настройки, предназначенные для размещения параметров настроек подключаемых к устройству дополнительных функций или устройств;
- электронный журнал, в который записываются критичные события и попытки НСД, зарегистрированные в системе;
- блок с учетными данными зарегистрированных пользователей.

Входящий в состав блока АПМДЗ блок функциональных модулей АПМДЗ включает в себя следующие программные модули:

- модуль контроля целостности;
- модуль диагностики состояния компонентов устройства;
- модуль контроля критичных интервалов времени процедуры запуска и загрузки компьютера;
- модуль настройки устройства;
- модуль идентификации модели материнской платы компьютера;
- датчик случайных чисел.

В качестве модулей взаимодействия с внешними СЗИ могут использоваться следующие:

- модуль загрузки ключевой информации в средства криптографической защиты информации (СКЗИ), включая абонентские и/или проходные шифраторы (в том числе, упомянутый выше криптографический сетевой адаптер «КРИПТОН AncNet», которым может быть оснащен управляемый сервер);
- модуль взаимодействия с установленной на компьютере системой разграничения доступа;
- модуль обеспечения сквозной аутентификации в операционной системе компьютера;
- модуль поддержки взаимодействия с серверами для проведения централизованного администрирования;
- модуль настройки устройства АПМДЗ-УС в части обеспечения возможности подключения к нему дополнительных устройств.

Все модули взаимодействия с внешними СЗИ являются опциональными. Их наличие необходимо только в случае подключения к устройству или установки в его операционной системе соответствующих СЗИ.

Программное обеспечение доверенной среды включает в себя следующие программные модули:

- ПО проверки целостности программно-контролируемых объектов и диалога с оператором;
- ПО удаленного управления устройством;
- доверенную ОС.

Второй из основных блоков устройства АПМДЗ-УС — блок управления ресурсами — включает в себя следующие компоненты:

- модуль доверенного соединения;
- модуль удаленного управления;
- модуль удаленной многофакторной взаимной аутентификации, предназначенный для удаленной аутентификации пользователя (администратора) на управляемом сервере;
- модуль, реализующий сетевой интерфейс Ethernet.

МДС представляет собой VPN-сервер, участвующий в формировании защищенного канала связи наряду с МДС в составе АРМ администратора.

Как было сказано выше, сервер и АРМ администратора могут быть оснащены устройствами «КРИПТОН AncNet», формирующими альтернативный, криптографически защищенный канал для передачи данных. В этом случае сервер и АРМ администратора становятся связаны двумя защищенными каналами, используемыми следующим образом:

The trusted boot unit includes the following components:

- local identification and authentication module that performs local user authentication and trusted computer loading;
- power management module that controls the main power of the computer (regardless of the chipset of the computer's motherboard) and locks the computer if the system detects violations;
- unit of functional modules performing the main functions of trusted loading;
- module of interaction with external (outside of the TBM-SM device) information security tools;
- trusted environment software;
- unit of settings of the TBM-SM device that contains a list of monitored hardware and software objects, settings and keys for centralized administration, as well as additional settings including the parameters of interconnection with the external information security hardware modules that are connected to the device;
- log-file that contains the registered information about critical events and attempts of unauthorized access;
- block with registered users credentials.

The unit of functional modules (that is part of the trusted boot unit) includes the following software modules:

- integrity control module;
- module of diagnostics of the device components state;
- module for checking critical time intervals of the computer starting and loading procedure;
- device configuration module;
- computer motherboard model identification module;
- random number generator.

The following modules can be used as modules of interaction with external information security tools:

- module for loading key information into cryptographic information security software or hardware, including several types of encoders (for example, the mentioned above cryptographic network adapter Crypton-AncNet that can be installed into the managed server);
- module of interaction with an access control system installed into the computer operating system;
- module providing the single sign-on of users into the computer operating system;
- module for supporting interaction with servers to provide the centralized administration;
- module for performing the setup of the TBM-SM device in terms of its interaction with external devices.

All modules of the unit described above are optional. Their presence is required only if the according information security hardware

- канал связи, сформированный модулями МДС на основе VPN-соединений, с программной защитой сетевого трафика, используется в рамках удаленного управления сервером;
- канал связи, сформированный устройствами «КРИПТОН AncNet», с аппаратным проходным шифрованием сетевого трафика, используется для передачи различной информации (например, содержимого файлов, хранящихся на управляемом сервере) в рамках информационного обмена между сервером и АРМ администратора.

МУУ отвечает за обмен данными между сервером и АРМ администратора в рамках удаленного управления.

Для обеспечения выполнения как основных функций АПМДЗ, так и функций удаленного управления серверами, устройство АПМДЗ-УС имеет следующие внешние интерфейсы:

- различные интерфейсы связи с компьютером, в качестве которых могут использоваться интерфейсы PCI, PCI Express (PCIe), USB и др.;
- интерфейс управления питанием компьютера и его блокировки, в качестве которого может использоваться любой проводной интерфейс;
- различные интерфейсы, обеспечивающие применение технологий удаленного управления сервером: serial-over-IP, KVM-over-IP, эмуляции USB-устройств и передачи информации датчиков состояний сервера (сенсоров) через Интернет;
- сетевой интерфейс Ethernet, на основе которого строится канал взаимодействия с АРМ;
- интерфейс связи с АНП (АНА), конкретный тип которого зависит от типа аутентифицирующего носителя;
- межмодульный интерфейс взаимодействия с устройством «КРИПТОН AncNet» и другие интерфейсы взаимодействия с внешними СЗИ, конкретные типы которых зависят от используемых СЗИ, например, межмодульный интерфейс (для загрузки ключей шифрования в аппаратные шифраторы), USB host (может также использоваться для подключения внешних устройств, в частности, считывателей смарт-карт или USB-идентификаторов), асинхронный последовательный интерфейс UART, например, RS-232 и др.

Разъемы данных интерфейсов могут быть выполнены как на плате самого устройства АПМДЗ-УС, так и вынесены на материнскую плату компьютера с целью минимизации габаритов устройства.

В качестве АНП или АНА могут использоваться электронные таблетки типа Touch Memory, смарт-карты различных типов, USB-идентификаторы и носители, карты памяти различных типов и т. п. Теоретически возможно использование биометрических признаков пользователей в качестве дополнительных факторов аутентификации. Следовательно, применяемый считыватель должен соответствовать типу используемого носителя:

- коннектор для электронных таблеток типа Touch Memory;
- интерфейс USB для USB-идентификаторов и носителей;
- контактный или бесконтактный (включая интерфейс ближнего поля NFC — Near Field Communication) интерфейс для смарт-карт;
- считыватель биометрических признаков и т. п.

Устройство АПМДЗ-УС может содержать подмножество из перечисленных выше блоков и программных модулей в зависимости от следующих факторов:

or software is connected to the TBM-SM device or is installed into the computer operating system.

The trusted environment software includes the following software modules:

- software for integrity check of program-controlled objects (it also provides the related GUI for administrators);
- remote device management software;
- trusted operating system.

The second of the main units of the TBM-SM device (the resource management unit) includes the following components:

- trusted connection module;
- remote management module;
- remote multifactor mutual authentication module intended for performing the remote authentication of the user (administrator) on the managed server;
- module that implements Ethernet network interface.

The TCM is a VPN server that participates in the provision of a secure communication channel along with the TCM module of the administrator's workstation.

As stated above, the server and the administrator's workstation can be equipped with Crypton-AncNet devices that form an alternative cryptographically protected channel for data transmission. In this case, the server and the administrator's workstation are linked by two secure channels that are used as follows:

- main communication channel created by the TCM modules and based on VPN connections with software protection of network traffic; it is used to provide the remote management of the server;
- alternative communication channel formed by the Crypton AncNet devices with hardware pass-through encryption of network traffic; it is used for transmitting various information (for example, the contents of files stored on a managed server) as part of the information exchange between the server and the administrator's workstation.

The RMM module is responsible for data exchange between the server and the administrator's workstation during the remote management.

To provide performing both the main functions of the trusted boot module and the remote server management functions, the TBM-SM device has the following external interfaces:

- various interfaces for communication with a computer, such as PCI, PCI Express (PCIe), USB, etc.;
- interface for computer power management and its locking, which can be any wire interface;
- various interfaces that provide the use of a variety of remote server management techniques, e.g.: serial-over-IP, KVM-over-IP, emulation of USB-devices and transmission of server components' state sensors information via the Internet;
- Ethernet network interface that allows building the channel of communication with the administrator's workstation;
- interface to AAC; its specific type depends on the type of authenticating carrier in use;
- inter-module interface to the Crypton-AncNet device and other interfaces for interaction with external information security hardware; types of such interfaces depend on the hardware used; for example, the inter-module interface for loading encryption keys into hardware encoders, USB host (can also be used to connect external devices, in particular, smart

- используемых в конкретной ИВС технологий;
- реализуемых устройством функций защиты;
- конкретного набора используемых внешних СЗИ.

Таким образом, выглядит возможным и перспективным использование созданного на базе устройства «КРИПТОН-ЗАМОК» устройства АПМДЗ-УС, сочетающего в себе функции, присущие аппаратно-программным модулям доверенной загрузки (защита от несанкционированного доступа, строгая аутентификация пользователей, контроль целостности программных модулей и формирование доверенной операционной среды), и функции по удаленному управлению серверами по защищенному каналу связи между управляемым сервером и АРМ администратора.

Основными особенностями функционирования компьютерной системы удаленного управления серверами на основе данного устройства являются:

- обеспечение надежной защиты ИВС и ее компонентов (сервера, АРМ администратора) на основе отечественных доверенных криптографических средств;
- проведение удаленной двухфакторной взаимной аутентификации;
- реализация удаленного управления серверами по защищенному прозрачно шифруемому каналу, обеспечивающему прохождение трафика с любыми стандартными протоколами и при использовании различных платформ и физических средств передачи и обработки информации.

Устройством «КРИПТОН-ЗАМОК» гарантируется доверенная среда, обеспечивающая повышение эффективности защиты компьютера от несанкционированных действий на всех этапах его работы, а также возможность удаленного администрирования и удаленной аутентификации в компьютерных сетях с различными протоколами передачи данных и используемыми платформами.

Благодаря широкой функциональности, а также выполнению наиболее критичных операций непосредственно в устройстве создания доверенной среды и осуществлению удаленного управления, устройство «КРИПТОН-ЗАМОК» с функциями удаленного управления серверами сохранило достоинства взятого за основу АПМДЗ, а именно, способность выполнять системообразующие функции и возможность построения комплексной системы для эффективной защиты компьютера и ИВС в целом. В то же время, данное устройство обеспечивает возможность удаленного администрирования и управления серверами при реализации надежной двухфакторной взаимной аутентификации, что повышает эффективность защиты и управления функционированием компьютерной сети.

Устройством «КРИПТОН-ЗАМОК» с функциями удаленного управления серверами целесообразно оснащать серверы, используемые в различных специальных применениях, в соответствии с которыми предъявляются повышенные требования к обеспечению информационной безопасности ИВС.

Авторы считают, что в данной работе новыми являются следующие результаты:

1. Предложены принципы создания систем удаленного управления серверами по криптографически защищенному каналу с использованием механизмов строгой аутентификации пользователей, осуществляющих удаленное управление.

card readers or USB tokens), asynchronous serial interface UART, for example, RS-232, etc.

The connectors of these interfaces can be placed both on the board of the TBM-SM device itself and on the motherboard of the computer in order to minimize the size of the device.

Several types of devices can be used as authenticating carriers, including i-Buttons, various types of smart cards, USB tokens and flash drives, various types of memory cards, etc. Also it is theoretically possible to use biometric attributes of users as additional authentication factors. Therefore, the reader must correspond to the type of media used:

- connector for i-Buttons;
- USB interface for USB tokens and flash drives;
- contact or contactless (including the NFC (Near Field Communication) interface) reader for smart cards;
- reader for biometric attributes, and so on.

The specific TBM-SM device may contain a subset of the above-mentioned units and software modules depending on the following factors:

- technologies used in a particular computer system;
- protection functions implemented by the device;
- specific set of external information security tools in use.

Thus, it seems possible and promising to use the TBM-SM device (created on the basis of Crypton-Zamok device) that combines the functions usually performed by trusted boot modules (unauthorized access prevention, strict user authentication, integrity control of software modules and creation of a trusted operating environment), and functions providing remote management of servers over a secure communication channel between the managed server and the administrator's workstation.

The main features of the server remote management system based on this device are the following:

- providing reliable protection of a computer system and its components (including the server and administrator's workstation) based on trusted boot modules and cryptographic devices or software;
- use of remote two-factor mutual authentication;
- implementation of remote management of servers over secure transparently encrypted channel that includes the traffic of any standard protocols on various platforms for information transmission and processing.

The use of the Crypton-Zamok device guarantees a trusted environment that provides an increase in the efficiency of protecting the computer from unauthorized actions at all stages of its operation, as well as the possibility of remote administration and remote authentication in computer networks with various data transfer protocols and used platforms.

Due to its wide functionality, as well as the fact that most critical operations on creating a trusted environment and implementing remote management are performed inside the device, the Crypton-Zamok device with remote server management functions has retained the advantages of the underlying trusted boot module, including the ability

2. Разработана функциональная схема устройства АПМДЗ-УС, совмещающего в себе основные функции, присущие аппаратно-программным модулям доверенной загрузки (такие, как идентификация и аутентификация пользователей, организация доверенной среды исполнения, контроль целостности программных модулей, контроль доступа к ресурсам защищаемого компьютера и др.), и возможности по удаленному управлению серверами по защищенному каналу связи.
3. Разработаны макетные образцы устройства АПМДЗ-УС и системы удаленного управления серверами.

В настоящий момент описанные выше технические решения (система удаленного управления серверами по криптографически защищенному каналу и устройство АПМДЗ-УС) находятся на этапе патентования [9, 10].

ЛИТЕРАТУРА

1. IPMI — Intelligent Platform Management Interface Specification Second Generation v2.0. — Document Revision 1.1, October 1, 2013 — Intel, Hewlett-Packard, NEC, Dell.
2. Minyard C. IPMI — A Gentle Introduction with OpenIPMI. // http://openipmi.sourceforge.net — Montavista Software, 2006.
3. Schneier B. The Eavesdropping System in Your Computer. // https://www.schneier.com — 2013.
4. Farmer D. IPMI: Freight Train to Hell or Linda Wu & The Night of the Leeches. // http://fish2.com — Version 2.0.3 — August 22nd, 2013.
5. Farmer D. Sold Down the River. // http://fish2.com — June 23rd, 2014.
6. Дударев Д. А., Полетаев В. М., Полтавцев А. В., Романец Ю. В., Сырчин В. К. Устройство создания доверенной среды для компьютеров информационно-вычислительных систем. Патент РФ на изобретение № 2538329 — ООО Фирма «АНКАД», 2014.
7. Дударев Д. А., Кравцов А. Ю., Полетаев В. М., Полтавцев А. В., Романец Ю. В., Сырчин В. К. Устройство создания доверенной среды для компьютеров специального назначения. Патент РФ на изобретение № 2569577 — ООО Фирма «АНКАД», ЗАО «Крафтвэй корпорейшн ПЛС», 2015.
8. Сетевые шифраторы «КРИПТОН AncNet». // http://www.ancud.ru.
9. Дударев Д. А., Панасенко С. П., Пузырев Д. В., Романец Ю. В., Сырчин В. К. Компьютерная система с удаленным управлением сервером и устройством создания доверенной среды и способ реализации удаленного управления. Заявление о выдаче патента РФ на изобретение № 2016144763 — ООО Фирма «АНКАД», 2016.
10. Бычков И. Н., Дударев Д. А., Молчанов И. А., Орлов М. В., Панасенко С. П., Пузырев Д. В., Романец Ю. В., Сырчин В. К. Компьютерная система с удаленным управлением сервером и устройством создания доверенной среды. Заявление о выдаче патента РФ на изобретение № 2017103816 — ООО Фирма «АНКАД», ПАО «ИНЭУМ им. И. С. Брука», 2017.

to perform backbone functions and the ability to build an integrated system for effective protection of computers and distributed systems in general. At the same time, this device provides the ability to administer and manage servers remotely while implementing reliable two-factor mutual authentication which increases the efficiency of protecting and managing functions.

It is advisable to use the Crypton-Zamok device with the functions of remote management of servers for servers meant for applications with increased requirements for information security.

CONCLUSION

The authors consider the following results of this paper to be novel:

1. The principles of creating systems for remote management of servers over cryptographically protected channels have been offered using mechanisms of strict user authentication before performing remote management.
2. The functional diagram of the TBM-SM device has been developed that combines the basic functions of trusted boot modules (such as identification and authentication of users, the organization of the trusted execution environment, control of the software modules integrity, access control to the resources of the protected computer, etc.) with the ability to remotely manage servers through a secure communication channel.
3. The prototypes of the TBM-SM device and the remote server management system have been developed.

At the moment, the technical solutions described above (the system for remote management of servers via a cryptographically protected channel and the TMB-SM device) are being patented [8, 9].

REFERENCES

1. IPMI — Intelligent Platform Management Interface Specification Second Generation v2.0. — Document Revision 1.1, October 1, 2013 — Intel, Hewlett-Packard, NEC, Dell.
2. Minyard C. *IPMI — A Gentle Introduction with OpenIPMI* // http://openipmi.sourceforge.net — Montavista Software, 2006.
3. Schneier B. *The Eavesdropping System in Your Computer* // https://www.schneier.com — 2013.
4. Farmer D. *IPMI: Freight Train to Hell or Linda Wu & The Night of the Leeches* // http://fish2.com — Version 2.0.3 — August 22nd, 2013.
5. Farmer D. *Sold Down the River* // http://fish2.com — June 23rd, 2014.
6. Dudarev D. A., Poletaev V. M., Poltavtsev A. V., Romanets Y. V., Syrchin V. K. *Apparatus for Creating Trusted Environment for Computers of Information Computer Systems*. Patent RU 2538329 — "ANCUD" Ltd., 2014. (In Russian).
7. Dudarev D. A., Kravtsov A. Y., Poletaev V. M., Poltavtsev A. V., Romanets Y. V., Syrchin V. K. *Device to Create Trusted Execution Environment for Special Purpose Computers*. Patent RU 2569577 — "ANCUD" Ltd., Kraftway Corporation PLC, 2015. (In Russian).
8. Setevye shifratory «KRIPTON AncNet». // http://www.ancud.ru.
9. Dudarev D. A., Panasenko S. P., Puzyrev D. V., Romanets Y. V., Syrchin V. K. *Computer System with Remote Control by Server and Device for Creating Trusted Environment and Method for Implementation of Remote Control*. Patent RU 2633098 — "ANCUD" Ltd., 2017. (In Russian).
10. Bychkov I. N., Dudarev D. A., Molchanov I. A., Orlov M. V., Panasenko S. P., Puzyrev D. V., Romanets Y. V., Syrchin V. K. *Computer System with Remote Control by Server and Device for Creating Trusted Environment*. Patent Application RU 2017103816 — "ANCUD" Ltd., PJSC "Brook INEUM", 2017. (In Russian).