ANALYSIS OF USERS WORK IN CLOUD COMPUTING ENVIRONMENT

U.A. Vishniakou, Z.R. Al-Attar Abdulraouf

Cloud computing (CC) have many advantages, but it is very important to ensure the safety of users and their recognition. Selected classes of threats in the CC environment related to the attacks: on the software; on cloud elements; on hypervisor, in the control system; threats of virtualization, migrate the virtual machines. The class of threats of users authority abuse, including due to the mutual influence of user tasks on computing nodes leading to unauthorized user access to data. Analysis of security mechanisms in CC systems showed that protection against joining unauthorized components is provided by means of mutual authentication mechanisms users and providers using digital certificates, encryption and digital signature of information transmitted between nodes of CC environments.

The main aspects of user security in CC. 1. Privacy, to achieve it, there are two main methods: physical separation and encryption. 2. Integrity: two main approaches to achieving it – message authentication code and digital signature. 3. Availability: make sure that users can access in Internet anytime and anywhere.

We consider the use of a new technology − Data-Centric Networking − DCS, which provides data owners with full control of their security throughout the life cycle of data in CC.

ANALYSIS OF USERS WORK IN CORPORATE MANAGEMENT SYSTEM AND E-SHOP

U.A. Vishniakou, H.J. Al-Musawi Hani, I.K. Nvosu

Traditional security paradigms in corporate management systems (CMS) provide security levels along the security perimeter: firewalls, intrusion prevention systems, encrypted network tunneling. Information-oriented network (ICN) is considered as a promising paradigm for the next generation of CMS working on Internet. In ICN content is more important than the host, which gives advantages such as reduced network load, low propagation delay, scalability, etc. Named Data Networking (NDN) represent the ICN architecture. The report presents four issues most important for security in NDN for information protection: from new forms of unknown attacks, privacy, blocking malicious network traffic, anomaly detection and DoS / DDoS attacks.

The following areas of protection in e-shops are highlighted: encryption method with digital signature, use of firewall, secure sockets layer (SSL), access permission. Encryption method: MD5 algorithm and password cache are used. Cache contains random data that are used as an additional login. A hash function hashes the password. The main function of cache is to protect against symbolic attacks against the list of hash passwords and against pre-computed attacks in the table. Firewall: creates an additional layer of security throughout the online store. With a firewall rule it will block attackers or blacklist them and deny access to the site. It has a scanner to provide installation recommendations in our e-shop. SSL protocol uses a 128-bit encryption key.

ANALYSIS OF THE BLOCK CHAIN USE

U.A. Vishniakou, R.Kh. Khudier

The functioning of the block chain and its security is provided by miners and other block chain participants. Access to the block chain takes place using special keys that guarantee the reliability of the entire network. Every user has it. A key is a set of cryptographic records. It is absolutely unique, which guarantees the impossibility of data substitution and hacker attacks. To do this, hackers need to access all the computers on the network. Mechanisms that ensure the efficiency and reliability of the block chain are algorithms of Proof of Work (PoW) – the work done, and Proof of Stake (PoS) – confirmation of the share. PoW in the block chain checks the calculations generated during the creation of a new block. The block is recognized as true and closed, provided that the value of its hash is less than the signature sought by miners. That is, a certain cryptographic cipher shows the authenticity of the block.

Examples of block chain application in various spheres of life, in addition to finance. Personal identification - services in the field of identification and confirmation of access rights work, which

create a digital equivalent of an identity card. Such startups include HYRP, BlockVerify, OneName and others. Copyright – the Ascribe platform uses the register in which artists, musicians, inventors can store the copyright of the encrypted identifiers. Management and law – already now there are projects like Borderless, which combine legal and economic services.

УГЛЕСОДЕРЖАЩИЕ ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Х.А.Э. Айад, О.В. Бойправ, Л.М. Лыньков

Авторами обоснована перспективность использования порошкообразных материалов на основе активированного, древесного и кокосового углей для создания электромагнитных экранов. Установлено, что значения коэффициента передачи электромагнитного излучения (ЭМИ) в диапазоне частот 0,7–17 ГГц экранов на основе порошкообразных углесодержащих материалов – не более –7 дБ (толщина экранов – 8 мм). Значения коэффициента отражения, измеренные в режиме короткого замыкания, достигают величины –10 дБ. Определено, что в результате пропитывания до насыщения порошкообразных углесодержащих материалов водным раствором хлорида кальция можно обеспечить снижение с –7 до –35 дБ значений коэффициента передачи и с –10 до –14 дБ коэффициента отражения ЭМИ электромагнитных экранов на их основе, что связано с увеличением с $4{,}6\cdot10^{-8}$–0,45 См/м до 0,1–70 См/м удельной проводимости таких порошков.

Таким образом, электромагнитные экраны на основе порошкообразных углесодержащих материалов могут быть использованы для обеспечения защиты информации от утечки по каналу побочного электромагнитного излучения, а также в целях снижения радиолокационной заметности наземных объектов.

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

В.М. Алефиренко

Подготовка специалистов по специальности «Техническое обеспечение безопасности», специализации «Технические средства защиты информации» осуществлялась в Белорусском государственном университете информатики и радиоэлектроники с 2002 по 2017 годы. Образовательная программа подготовки специалиста предусматривала изучение циклов социально-гуманитарных, естественнонаучных, общепрофессиональных и специальных дисциплин, дисциплин специализации, факультативные дисциплины, экзаменационные сессии, три вида практик, дипломное проектирование и итоговую государственную аттестацию [1]. Цикл общепрофессиональных и специальных дисциплин включал в себя обязательный компонент, вузовский компонент и дисциплины по выбору. Цикл дисциплин специализации включал в себя такие дисциплины как: «Первичные измерительные преобразователи и их применение в системах обеспечения безопасности», «Физические и аппаратные средства защиты информации», «Техническая защита информации в каналах утечки и вычислительных системах и сетях», «Технические и программные средства защиты информации в офисных и банковских системах» и «Проектирование электронных средств и систем обеспечения безопасности». Обучение студентов по специальности «Техническое обеспечение безопасности» предусматривало как очную (дневную), так и заочную формы обучения. При дневной форме обучения срок подготовки специалиста составлял 5 лет, а по заочной форме обучения увеличивался на 1 год. В университете осуществлялась также подготовка специалистов по заочной форме обучения для получения высшего образования, интегрированного со средним специальным образованием, что сокращало время подготовки до 4 лет. Подготовка специалистов проводилась как на бюджетной, так и на платной основе. Выпускающей кафедрой являлась кафедра «Проектирование ннформационно-компьютерных систем». При подготовке специалистов по специальности «Техническое обеспечение безопасности» использовались различные виды инновационных технологий, включая собственные разработки университета. За весь период подготовки по всем формам обучения по специальности «Техническое обеспечение безопасности» в Белорусском государственном