DEFENSE TOOLS IN CORPORATE INFORMATION SYSTEM, CLOUD COMPUTING AND BLOCKCHAIN

Belarusian State University of Informatics and Radioelectronics
Minsk, The Republic of Belarus

AL-MUSAWI HANI H.J., AL-ATTAR ABDULRAOUF Z.R., KHUDIER R.K.

Vishnyakou U.A. – doctor of techn. science, professor

Annotation. The analysis of tools in corporate information system, cloud computing and blockchain are given. Some elements of such as neural net, multi-agent systems are discussed.

The main sources of information about the state of corporate information system (CIS) elements that are important for the task of detecting attacks are identified: event logs and information about processes occurring on CIS servers, router logs, packets, transmitted over the network, event logs and information about processes occurring on workstations. The model of multi-agent IDS is considered, which includes a set of interacting intelligent agents, information system components, and sources of information to be analyzed for the task of detecting attacks [1].

The structure of the protected network of the CIS is presented. The server is running Slack ware Linux 10.2 with the kernel version 2.4.31. This version of the kernel is the most researched, stable, and contains the minimum number of vulnerabilities detected. The server is protected using the IPtables firewall (v1.3.3). The result of combining IDS Snort and ITU IPTables is a two-level security system: at the first level, IPTables checks the incoming packet for compliance with its filtering rules, if the packet has received permission to pass through the firewall, it is checked by the intrusion detection system for the presence of malicious code in the body of the incoming packet.

The neural networks structure using for task solving of information defense are discussed. The choice of attribute and metadata of executing files with two states (clean and with viruses) which used for multilevel perceptron teaching are built. The teaching was realized within SPSS Statistics – program of IBM Company. After the teaching of neural network the efficiently its working with the control choice of executing files was determined.

The main threats to the cloud computing (CC) environment are: virtual machine system (VMS) are dynamic, they are cloned and can «move» between physical servers, which affects the development of security integrity; CC servers and local physical clusters use the same OS and applications, which increases the «attacked surface»; when the VM is turned off, it is at risk of infection; when using CC, the network perimeter is blurred or disappears, which leads to the fact that the protection of the less secure part of the network determines the overall level of security; to protect against functional attacks, the following security measures must be used for each segment of the OV environment: for the domain controller server, effective protection against DoS attacks, for the Web server, page integrity control, for the application server, application-level screen, for the data storage system, backup, access control; most users connect to the cloud using the browser (Cross Site Scripting attacks, password theft, browser session hijacking, man-in-the-middle attacks, etc.).). A large number of VMS requires management systems that can be tampered with to block the operation of the VM; an attack on a hypervisor can lead to one VM being able to access the memory and resources of another [1].

The problem of validation. Transactions related to mechanisms for confirming authorship or authenticity using the digital equivalent of a document are used to present proof of one party to the other. The validator verifies the hash value, the transaction timestamp, and the identity of the bearer record. The mechanism for automated document validation based on the use of blockchain covers only two parties (the bearer and the verifier), which is not sufficient in the case of official documents, the issuer of which must be present in the model as a trusted third party. The confirmation model must establish not only that the document belongs to the issuer, but also confirm the issuer's authority to carry out this type of activity and additional information (for example, for the education sector, lists of training specialties for a certain period of time in accordance with the license.

The report considers the threats of IS to the CIS, and suggests using the technology of multi-agent systems to protect the perimeter of the corporate system. We consider the threats of IS for the cloud environment, and suggest using neural network technology to protect against malware that can be used in the SaaS model. The mechanisms of blockchain technology with information protection through

encryption and hashing of lists of distributed registers are considered. It is proposed to use this technology in education for document control.

List of literature sources:

1. Vishniakou, U.A. Information security in corporate systems, electronic commerce and cloud computing: methods, models, hard-software tools. Monograph / U.A. Vishniakou. – Minsk, Bestprint, 2016. – 276 p.