Elements of Information Security in Integration Corporate Information System on Base of Intelligence Technologies Use

Vishniakou U.A., Gondagh Sas M.M., Mozdurani M.G. Shiraz
Belorussian State University
of Informatics and Radioelectronics,
Minsk, Republic of Belarus
Email: vish2002@list.ru

***Abstract*—The main directions of information security when using intelligent technology are done. The uses of information security (IS) of corporate information system (CIS) using clouding computing (CC). The conception of integrated CIS is introduced. The model of ICIS using multi-agent technology is proposed. The main problems of information security ICIS are analyzed, authentification user mechanisms are shown, its models and algorisms are done.**

***Keywords*—intelligent technology, information security, authentification mechanisms.**

I. Introduction

The IS situation is following: the present stage of development of the theory and practice of support IS – on the one hand, the reinforced attention to safety of information objects, increase in requirements for information defense (ID), acceptance of the international standards in information security field, the growing expenditures on protection support, with another – the increasing damage caused to owners of information resources what the published data on damage to world economy from the hacker attacks confirm [Vishnyakou, 2014].

Output is implementation at all stages ID the intellectual technologies acquiring the increasing distribution in ID systems. On the one hand, data collection and processing from the Internet about a status, the direction of development and level of threats of processes in the world community and synthesis of knowledge, the reflected in sources, realized on the basis of their intellectual processing, gives the new integrative quality allowing to predict, simulate and prevent development of security risks. On the other hand, the use of intellectual technologies of data handling gives an opportunity to raise the security level of different corporate information systems (CIS) and platforms of the cloud computing (CC) [Molyakov, 2014]. Development of technologies and environments of cloud computing (ECC) enters new sources of threats which need to be considered in case of safety of computer systems and services. The tendency of ECC use in CIS of organizations is entered [Ridz, 2011]. 2014].

II. The directions of intellectualization in ID

Intellectual systems of ID (ISID) providing detection of the attacks as the intelligent tool use the neural networks (NN), systems of a fuzzy logic and, based on rules, the expert systems (ES). If NN is presented in the form of the separate system of attack detection, then in case of traffic handling there is an information analysis on existence of abuses. Cases with specifying on the attack are redirected to the administrator of safety. This approach is high-speed as one level of the analysis is used. One of the main shortcomings of NN is «opacity» of formation of analysis results [the Kalatch, 2011].

In the knowledge base (KB) of ES contains the description of classification rules to the appropriate profiles of legal users and scenarios of attacks to CIS. ISID shortcomings on the base of ES are: the system isn't the adaptive and not always the unknown attacks are found. In systems of attack detection it is possible to select application of the neural networks added by ES. Sensitivity of system increases as ES obtains data only on events which are considered as suspicious. If the neural network due to training began to identify the new attacks, then expert system KB is necessary to update [the Kalatch, 2011].

Use of hybrid neuro-expert or neuro-fuzzy systems allows to reflect fuzzy predicate rules which are automatically adjusted in training activity of a neural network in structure of system. Property of adaptively of fuzzy NN allows to solve separately the taken problems of identification of threats, comparisons of behavior of users to the templates which are available in system, to automatically create new rules in case of change of threat field [the Kalatch, 2011].

Shortcomings of these systems are: need of presence of high qualification experts; the difficulties arising in case of adaptation of methods to needs of the specific organization; impossibility to estimate efficiency of the specific complex of security features applied on subject to protection; the requirement of existence at the enterprise of authentic statistics on incidents of information security.

III. The concept of integrated CIS

Development of technologies and the environments of ECC enter new sources of threats which need to be considered in case of safety of computer systems and services. The tendency of use of ECC was outlined in CIS of organizations, integrated CIS (ICIS). The dynamic nature of processes of information exchange complicates possibilities of operational assessment of risks of violation of confidentiality, integrity and accessibility of the program and infrastructure resources provided in the mode of remote access. In the report structures of ICIS, model for information identification in ICIS and the concept of intellectual system of support of its information security are considered.

Let's separate ICIS on technologies of CC application: small – on the basis of SaaS, averages – on the basis of IaaS, big on the basis of PaaS. Most the enterprises will work on hybrid model, providing and consuming cloudy services which will be integrated if necessary into the IT traditional models. The new model of information systems is created: instead of installation of application packages on the computers the companies will use browsers to get access to the wide range of the cloudy services available according to the first requirement. Rent of cloudy services allows: to carry the expenditures connected to use of IS to variables, but not constant expenses; to create the analysis systems of data displaying operation of the enterprise, integrating data from separately CRM and ERP systems; to create prototypes of new products and innovative projects, developing interaction between employees, overcoming boundaries of the organizations and states.

The directions of development of ID in ICIS can be defined as following [Vishnyakou, 2014]:

- development of models of violation and counteraction of ID in ICIS on the basis of a choice of an optimal variant of response to safety events;
- enhancement of ID system architecture for ICIS providing effective management in the conditions of uncertainty of a status of the information environment;
- enhancement of instrumental program complexes with intellectual support of decision-making with a research of efficiency of methods, models and algorithms;
- development of technologies the multi agent of systems for detection of the attacks, counteraction to threats of violation of ID, assessment of level of security of information in ICIS;
- development of models and security features of ICIS on the basis of a cloud instrumental platform of design of the ISID on the basis of semantic technologies.

IV. Information security models in ICIS

Input of the model considering dynamic character of resources and structure of protocols of network interaction is the flow of network packets which come to ID system fire-walls in the environment of CC, and an output is division of packets into the virtual connections, classification of everyone is this on accessory to connection and determination of a subset of rules of filtering for them. Model of counteraction to threats of ID in CIS in which the decision on option of reaction is made depending on probability of the attack estimated with use of the mechanism of fussy logical output [Mashkina, 2009].

For development of the ID models in ICIS it is offered to use object algebra (OA) [Vishnyakou, 2014]. In OA the description of carriers and communicators objects in computing environment are shown, also the abstraction layers of objects are developed; representation the unlinked, parallel, competing objects at one abstraction layer is done; the description developing, paused, created, nonexisten objects are entered that allowed to show that the main disjuncts (rule, fact, request, empty one) are similar to these types of objects [Vishnyakou, 2014]. In the ID models objects are transformed to models of agents. In a general view we will present the ID model in ICIS in the form:

$$M_{ik} = (M_t, M_a, M_s, M_p),$$

where M_t – model of detection of threats, M_a – model of user authentication, M_s – the model of the analysis and assessment of a software (allowing to receive an output about existence or absence of its destructive properties), M_p – model of counteraction to threats.

Taking into account multyagenthy approach this model is transformed to the following look:

$$M_{ik} = (A_t, A_a, A_s, A_{ta}, A_p, A_c),$$

where A_t – agents of detection of threats, A_t – agents, the users differentiating access rights, A_s – agents of the analysis and assessment of a software, A_{sa} – agents determination attack type, A_p – agents, the attacks building the scenario of behavior for reflection, A_c – agents coordinators of all multyagenthy system. For small ICIS this model will be reduced to a type:

$$M_{ik} = (A_a, A_s, A_p, A_c).$$

V. Models of authentication of users in ICIS

In article [Vishnyakou, 2016] approach elements for safe operation of users in the environment of CC are provided. Participants of interactions: the user (as users there can be persons and the organizations), an authenticator of trusty (Trusted Authenticator – TA), cloud provider of services (Cloud Service Provider – CSP), the digital signature (DS), the agent of CSP's. Functions of elements of this approach are given below.

1) The user has limited access to services from a cloud of the offered services, he requests cloudy resources from CSPs.
2) TA connection establishes trusting relationships with an authentication organ. The task TA in the cloudy environment – to provide to the user safe access to cloud services through service provider.
3) The cloud service can dynamically be scaled for satisfaction of needs of users because the service provider provides the equipment necessary for service, and the software.
4) The digital signature (DS), is the digital signature which identifies the identity of the message sender or signed the document, and certifies that original contents of the sent message or the document, didn't change.
5) The agents of CSP's are capable to make decisions on execution of tasks on behalf of the users. Agents have the right to interact with other agents by negotiations, cooperation and coordination. In CSP the agent works for rendering of services, service of negotiations, services of cooperation and their coordination.

Let's expand this model: X – user, Y – authenticity authenticator. For the description we will enter designations: t_x – time tag, r_x, r_y – random numbers X and Y respectively;

S_x, S_y – the signatures generated by X and Y; S_{koh}, S_{kou} – certificates of public key of X and Y. Let's give authentication algorithms.

1) One-sided authentications using time stamps:

   $X \to\ Y : C_{koh},\, t_x,\, I_x,\, S_x(t_x, I_x)$

   After acceptance of the message the authenticator of trusty checks correctness of time tag t_x, the got I_x ID, and using public key from the certificate S_{koh}, the correctness of the digital signature $S_x(t_x, I_x)$.

2) One-sided authentications using random numbers:

   $Y \to X,\ r_y$ Y (1); $X \to Y:\ C_{koh},\ r_x,\ I_y,\ S_x(r_x, r_y, I_x)$ Y (2).

   The authenticator of trusty sends to the user the X random number of r_y. based on the message from X. Using public key X from the certificate S_{koh}, Y checks the correctness of the signature of $S_x(r_x, r_y, I_x)$ under r_x number, r_y number received in the first message and its I_x identifier.

3) Double-side authentications using random numbers:

   $Y \to X,\ r_y$ (1); $X \to Y:\ C_{koh},\ r_x,\ I_y,\ S_x(r_x, r_y, I_x)$ (2); $Y \to\ X : C_{koy}, I_x, S_y(r_x, r_y, I_x)$ (3);

   In this algorithm message handling 1 and 2 is executed as well as in previous one, and the message 3 is processed similar to the message 2.

VI. Authentication algorithms

In the authentication server for authentication of the user and a cloudy Web-server providing services to the user the sequence of actions is executed.

1) The user enters the information for registration.
2) The system of the user sends them as input data to a Web-server.
3) The server of authentication generates one time code and sends to a mobile application.
4) The user enters this code as a contribution during session time as after user session shall log in again.
5) After successful login, the user can get access to resources.

Steps of an algorithm of user authentication for registration in the cloudy environment through a mobile application the following.

1) The user clicks on the registration button on the page of the website.
2) Goes request to the Web-server for registration.
3) The Web-server creates the login page and returns it.
4) The user enters authentification information.
5) The user clicks the registration button.
6) Information on the user is transferred to the Web-server.
7) The Web-server checks information for correctness (validity) of filling and creates filling errors.
8) The Web-server returns filling errors to the user
9) The user makes corrections and again sends information to the Web-server.
10) The Web-server confirms a filling correctness
11) The Web-server saves information.
12) The Web-server transfers the message on the carried-out registration for e-mail.

VII. ID architecture conception

The ID architecture includes system of input of influences, the knowledge base on the basis of rules of production and frames, the solver with use of an inference engine, the basis of agents, the communication medium with agents, the coordinator.

For the task of detection of the virus attacks, the system of influence input transfers the facts about external influences to the knowledge base. The solver inference-based works out the decision which is transferred to the coordinator about changes of an external environment. For the distributed decision the coordinator can use their different types from a basis of agents: subcoordinator, performers, integrator.

Agents can be connected among themselves in the form of multi-level architecture. Such multi-level architecture of agents is suitable for the decision of the task of detection of the virus attacks. Taking into account specifics of the solvable task the multi agent architecture shall include several types of agents which perform different functions. In an analysis result of information process of detection of the virus attacks on the ICIS networks it is possible to consider such agents: authentications of net surfers, detection of the attacks, determination of their types building the scenario of behavior for reflection of the virus attack which is the subcoordinator of all multi agent architecture.

(Expanded) solutions on an instrumental platform on the basis of multi agent technology are proposed [Vishnyakou, 2016]:

- the development of structure of the multi agent system of detection of the attacks including agents of workstations, servers, routers, a hypervisor and allowing to draw a conclusion about the attacks, a status and perspectives of its protection;
- receiving a method of acceptance by agents of the joint decision allowing to create communication of agents and based on analysis results of the data received from different sources, to estimate CC condition in general;
- the framing of a technique of detection of the attacks with use the multi agentny of technologies allowing to train multi agentny system and to use it for further detection of unknown influences of CC.

Such to an instrumental platform the designer of option includes, library of agents, the rule base, a basis of methods. Based on the description of requirements to ID option the designer generates system option for specific ICIS.

VIII. Conclusion

The direction in szi is development of models, methods, architecture and hardware and software of control of zee for the solution of the problem of protection of pussycats and the cloud instrumental platform of design of intellectual systems on the basis of semantic technologies.

Approach for safe operation of users in the environment of cloud computing is given. Participants of interactions: the user (to users there can be natural persons and the organizations), the authenticity authenticator, cloud provider of services – csp, the sign-code signature – ds, the agent of csp's. The model and autentifikafiya's algorithms, the concept of architecture of ib is provided.

References

[1] [Vishnyakou, 2014] Vishnyakou, U. A. Information control and safety: methods, models, hardware-software decisions. Monograph. / U. A. Vishnyakou. – Minsk: MIU, 2014. – 287 p.

[2] [Molyakov, 2014] Molyakov, Ampere-second. Models and a method of counteraction to the hidden threats of information security in the environment of cloud computing/Ampere-second. Molyakov / Abstract PhD thesis. on specialty 05.13.19. SPb, 2014. – 17 p.

[3] [Ridz, 2011] Ridz, J. Cloud computing. / J. Ridz / – With, St. Petersburg: BHV, 2011. – 288 pages.

[4] [Kalatch, 2011] Kalatch, A.V., Nemtin E. S. Intellectual means and simulation of systems of information security the Online magazine "Tekhnologii Tekhnosfernoy Bezopasnosti" Release No. 3 (37) – 2011. – Pp. 3-11.

[5] [Vishnyakou, 2016] Vishnyakou U. A., Means of authentication of users in enterprise systems of control and the environments of cloud computing / Vishnyakou U. A., M. M. Gondagh // Reports of BGUIR, 2016, No. 3. – Pp. 94-97.

ЛЕМЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННОЙ КИС НА БАЗЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

Вишняков В.А., Гондаг Саз М.М., Моздурани М.Г
Шираз

Показаны основные направления защиты информации при использовании интеллектуальных технологий. Введено понятие интегрированной КИС. Представлены направления использования информационной безопасности (ИБ) КИС с использованием ОВ (ИКИС). Предложены модели ИБ в ИКИС с использованием многоагентных технологий. Проанализированы основные проблемы информационной безопасности ИКИС, рассмотреы механизмы аутетификации пользователей, представлена ее модель и алгоритмы.