Model of a Secure Virtual Environment for Managing Information Exchange in Scientific and Educational Organizations

Sergey Lazarev [1] and Konstantin Rubtsov [1]

[1] *Belgorod State University, 85 Pobedy Street, Belgorod, 308015, Russia*

Abstract

In this paper, the authors highlight the issues of constructing a set-theoretic model for the administration of information exchange in a protected virtual environment in the interaction of scientific and educational organizations. Based on the description of relations between entities and rules of information exchange, a method is proposed for describing the composition, structure of classes and their hierarchy, which make it possible to represent the object a model of information interaction within the framework of a unified management and security policy. A model of session access to information resources of a network of corporate portals has been developed.

Keywords

Administration of information exchange, secure virtual environment, object system model, description of object models

1. Introduction

Currently, the dominant methodology used in the development of applications and information systems is the object-oriented approach. In this paper, the authors consider a model of the relationship of entities when describing the virtual environment of information interaction of scientific and educational organizations. The main link of interaction is the portal, which is considered as a set of interconnected sections (access objects) with a hierarchical tree structure of subordination. For each section of the portal, only one access rule can be assigned, which applies to the entire branch of the object tree due to the mechanism of inheritance by child objects of the access rights of the parent object. For a child object, the rights inheritance mechanism can be disabled, and new access rules can be assigned, which will be inherited by its descendants. Set theory and mathematical logic are used as a mathematical apparatus for describing a set-theoretical model of a protected virtual environment for information interaction between scientific and educational organizations [1, 2]. The protected virtual environment is built based on the existing hardware and software infrastructure using public portals and communication channels, that is, it is a completely virtual structure of information interaction [3, 4].

2. Development of a secure virtual environment model for the administration of information exchange in the scientific and educational organizations

The authors have developed a model of a secure virtual environment for managing information exchange in scientific and educational organizations. A full description of the model, an assessment of its effectiveness, occupy more than a hundred pages of text. Due to the limited volume of publication, only the main points of the development of the model are given below.

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia

EMAIL: lazarev_s@bsu.edu.ru (Sergey Lazarev); rubtsov@bsu.edu.ru (Konstantin Rubtsov)
ORCID: 0000-0001-6584-9871 (Sergey Lazarev); 0000-0002-6408-3621 (Konstantin Rubtsov)

2.1. Problem determination

To build a model of a secure virtual environment for the administration of information exchange of scientific and educational organizations, it is necessary to map into the information space the elements and their interconnections of the organizational and technical association of the subjects of information interaction within the framework of associations, consortia or network structures implementing joint projects and solving common problems.

When creating such a mathematical model, there is a problem of applying the classical concept of the set-theoretic apparatus, implying a single instance of each element of the set. This does not provide a simple description of the elements of the secure virtual administration environment [8, 9, 14, 15].

2.2. Methods

Consider regulatory bodies, external actors, members of the association and their units, employees, as well as a security policy defined for each subject as subjects of information interaction within associations, consortia or network structures. For real (physical) subjects of information interaction, the main entities can be identified that describe their characteristics as a set of subjects ***O***. This set is reflection onto a set ***P***, which is a set of virtual objects that exist only within the protected environment, represented by Figure 1.

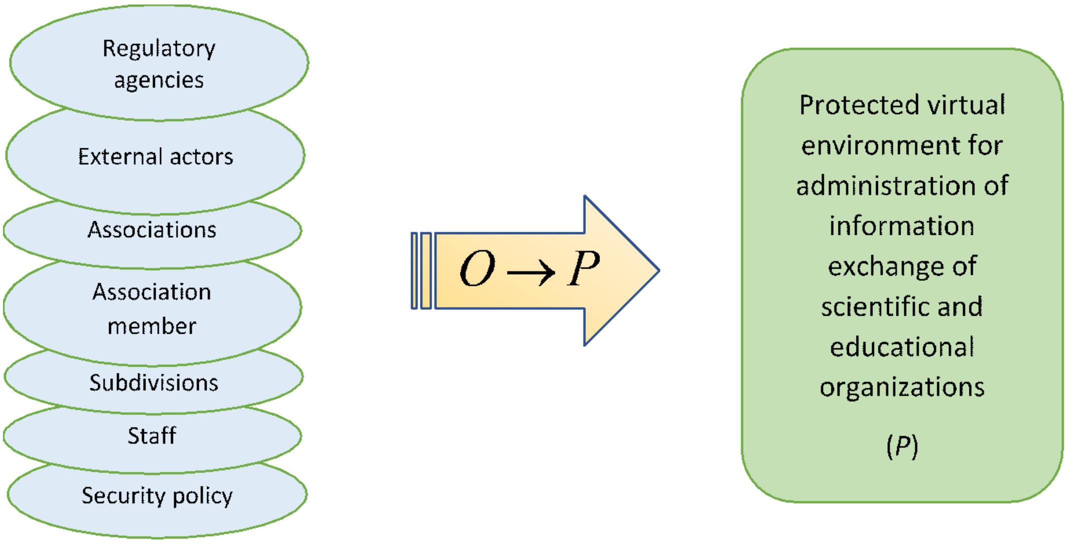


Figure 1: Reflection the elements of information exchange of scientific and educational organizations into a secure virtual environment of administration

Thus, a secure virtual environment provides the integration of heterogeneous distributed information and computing resources belonging to different subjects, under the control of a single administrative center that implements the functions of secure information interaction within the framework of a single management model and security policy [10, 12, 13].

2.2.1. Mathematical methods

The work uses a relatively new concept of a multiset, which is an extension of the classical definition of a set and allows the inclusion of the same element in the set several times. The concept of a multiset is actively used in computer science, artificial intelligence, and decision theory. Description of database elements, access rights and their interaction, description of string data, arrays, database elements, requires entering indices (identifiers), which assumes an unambiguous position of elements in some sets. In computer science, for this purpose, the concept of "tuple" is introduced into mathematical formalism, corresponding to an ordered set of fixed length. Within the framework of set theory, tuples can be inductively associated with sets [5].

2.2.2. Description of the main subjects of information interaction

The authors in this paper denote sets, multisets, and tuples in uppercase letters, and their elements in lowercase.

The set of subjects and entities $\boldsymbol{O}$ of information interaction within associations, consortia or network structures of scientific and educational organizations, together with a set of virtual objects $\boldsymbol{P}$, form a protected virtual environment of their interaction, which is a set $\boldsymbol{S} = \{ \boldsymbol{O} , \boldsymbol{P} \}$, while the set of objects $\boldsymbol{O}$ is an injection into $\boldsymbol{P}$: $\boldsymbol{O} \rightarrow \boldsymbol{P}$. The authors define the sets $\boldsymbol{O}$ and $\boldsymbol{P}$ as tuples, the elements of which are sets of typed data, tuples, or multisets.

The authors have defined the basic elements of the $\boldsymbol{O}$ and $\boldsymbol{P}$ tuples: $\boldsymbol{O} = < \boldsymbol{o}_i >$, $i = 1..7$; $\boldsymbol{P} = < \boldsymbol{p}_j >$, $j = 1..10$, where $\boldsymbol{o}_1$ – regulatory bodies, $\boldsymbol{o}_2$ – external actors, $\boldsymbol{o}_3$ – associations, $\boldsymbol{o}_4$ – members of the association, $\boldsymbol{o}_5$ – divisions of the association, $\boldsymbol{o}_6$ – employees of the division of the association, $\boldsymbol{o}_7$ – security policy of the association, $\boldsymbol{p}_1$ – institution, $\boldsymbol{p}_2$ – management server, $\boldsymbol{p}_3$ – access server, $\boldsymbol{p}_4$ – user domain, $\boldsymbol{p}_5$ – portal resource, $\boldsymbol{p}_6$ – access sections, $\boldsymbol{p}_7$ – access level group, $\boldsymbol{p}_8$ – access rights, $\boldsymbol{p}_9$ – account, $\boldsymbol{p}_{10}$ – site request.

The elements of the $\boldsymbol{O}$ and $\boldsymbol{P}$ tuples contain a description of the structural elements and methods of information interaction between research and educational organizations in a secure virtual administration environment. The authors performed a description of all elements (about 200) of the $\boldsymbol{O}$ and $\boldsymbol{P}$ tuples, including:

- description of the set of subjects of the protected virtual environment;
- description of the set of regulatory documents;
- a description of the set of elements of the protected virtual environment;
- mathematical description of the relationship between objects of the protected virtual environment.

For example, for $\boldsymbol{o}_4 = < \boldsymbol{o}_{4i} >$, $i = 1..5$, where $\boldsymbol{o}_{41}$ – tuple with the names of union members, $\boldsymbol{o}_{42}$ – tuple with an identifier of a union member, $\boldsymbol{o}_{43}$ – tuple with a legal address, $\boldsymbol{o}_{44}$ – tuple with bank details, $\boldsymbol{o}_{45}$ – tuple with the roles of members of the association.

2.2.3. An example of a description of the interaction of individual objects in a protected virtual environment

Let us consider as an example of a mathematical description of the model of interaction between individual objects of the virtual environment for the administration of information exchange of scientific and educational organizations and the execution of session authentication requests [6, 7, 11].

When performing session requests with authentication in the portal, it can be formally defined as a tuple $\boldsymbol{H} = < \boldsymbol{A}, \boldsymbol{C}, \boldsymbol{D} >$, where $\boldsymbol{A} = \{\boldsymbol{a}_i\}$ – set of access control nodes $\boldsymbol{A} \in \boldsymbol{P}_3$, $i = 1..n$; $\boldsymbol{C} = \{\boldsymbol{c}_j\}$ – set of network control nodes $\boldsymbol{C} \in \boldsymbol{P}_2$, $j = 1..m$; $\boldsymbol{D} = \{\boldsymbol{d}_i\}$ – set of user domains in the $\boldsymbol{D} \in \boldsymbol{P}_4$ network. A custom domain means a uniquely named group of users, which is represented by a tuple: $\boldsymbol{d}_j = < \boldsymbol{U}_i, \boldsymbol{D'}_i >$, where $\boldsymbol{U}_i$ – set of users of the $\boldsymbol{i}$-th domain, $i = 1..n$, $\boldsymbol{D'}_i$ – subset of domains in the network with trusted domain relations $\boldsymbol{d}_j$, $\boldsymbol{D'}_i \subseteq \boldsymbol{D}$ and $\boldsymbol{d}_i \in \boldsymbol{D'}_i$. Each user domain corresponds to a specific network access control node and vice versa, $\boldsymbol{A} \leftrightarrow \boldsymbol{D}$. In each user domain $\boldsymbol{d}_j$, there is a subset of currently authorized users $\boldsymbol{U'}_i \subset \boldsymbol{U}_i$. The network control node is a tuple $\boldsymbol{c}_j = < \boldsymbol{S}^0, \boldsymbol{R}^0, \boldsymbol{D} >$, where $\boldsymbol{S}^0$ – set of all active user sessions of the portal network; $\boldsymbol{R}^0$ – set of all identified requests on the network.

An access control node can be represented as a tuple: $\boldsymbol{a}_i = < \boldsymbol{S}_i, \boldsymbol{R}_i, \boldsymbol{D'}_i >$, where $\boldsymbol{S}_i$ – set of active users of the access control node's sessions, $\boldsymbol{R}_i$ – set of identified requests to the access control node. Session Access Model:

$$\forall\ \boldsymbol{a}_i : \exists\ \boldsymbol{s}_{ik} \in \boldsymbol{S}_i , \boldsymbol{u'}_{qz} \in \boldsymbol{U'}_q , \boldsymbol{d}_q \in \boldsymbol{D'}_i \Rightarrow \boldsymbol{T_f} : \boldsymbol{s}_{ik} \rightarrow \boldsymbol{u'}_{qz} , \qquad (1)$$

where $\boldsymbol{a}_i$ – access control node, $\boldsymbol{u'}_{qz}$ – the z-th authorized user of $\boldsymbol{s}_{ik}$ session of $\boldsymbol{d}_q$ domain, $q = 1..n$, $\boldsymbol{T_f}$ – function of matching the user and his session.

A user request for a secure virtual information interaction environment is considered identified when it is possible to determine its initiator based on condition (1) for an active session:

$$\forall \; \boldsymbol{r}_{ikx} \in \boldsymbol{R}_i : \exists \; \boldsymbol{s}_{ik} \in \boldsymbol{S}_i \Rightarrow \boldsymbol{E} : \boldsymbol{r}_{ikx} \rightarrow \boldsymbol{s}_{ik}, \qquad (2)$$

where $\boldsymbol{r}_{ikx}$ – is the request x to the i-th node containing the label k of the user session, $\boldsymbol{E}$ – function of identifying the user session on request, and the relation $\boldsymbol{F}_A$ determining the permission of the user to access the resource: $\exists \; \boldsymbol{F}_A : \boldsymbol{U} \times \boldsymbol{R} \rightarrow \{true, false\}$.

Thus, to identify a user session (2), it is necessary and enough to have session data only on the access control node that processes the request.

Objects of access to information resources of the protected virtual environment for the administration of information exchange of scientific and educational organizations will be called sections $\boldsymbol{P}_6$. Each section of the $\boldsymbol{q}_z$ network has a unique identifier z, so the set of sections $\boldsymbol{Q}$ can be represented as follows [4]:

$$\boldsymbol{Q} = \{ \boldsymbol{q}_z \}, \; z \in \boldsymbol{Z} \;, \qquad (3)$$

where $\boldsymbol{Z}$ – set of identifiers of sections of the corporate portal network.

Each access object, except for the root one, which is considered the portal itself, has a single parent object and any number of child objects.

Each section $\boldsymbol{q}_z$ is characterized by one or another access level $\boldsymbol{n}_z$, based on which the access rights to the corresponding information resources are established. The minimum level of access to the section of the corporate portal network is set by the number 0, the maximum – by the number M.

The set of all registered users of the corporate portal network can be represented as a set $\boldsymbol{Y}$. The elements of the set $\boldsymbol{Y}$ are users $\boldsymbol{u}_w$:

$$\boldsymbol{Y} = \{ \boldsymbol{u}_w \}, \; w \in \boldsymbol{W} \;, \qquad (4)$$

where w – unique identifier of the user $\boldsymbol{u}_w$; $\boldsymbol{W}$ – set of corporate portal user identifiers.

One of the main attributes of the $\boldsymbol{u}_w$ user is his $\boldsymbol{m}_w$ access level, which determines the privileges of this user in working with sections of the corporate portal network. The user access level $\boldsymbol{m}_w$ can take on a certain value from the set $\{ 0, 1, \dots, M \}$. The higher the value of $\boldsymbol{m}_w$, the more access rights to sections of the corporate portal network user $\boldsymbol{u}_w$ has.

To group users according to the level of their privileges (access rights) in the system, access privilege groups are used. The set of such groups can be represented as a set $\boldsymbol{G}$, whose elements are the privilege groups $g_0, g_1, \dots, g_M$:

The set of all registered users of the corporate portal network can be represented as a set $\boldsymbol{Y}$. The elements of the set $\boldsymbol{Y}$ are users $\boldsymbol{u}_w$:

$$\boldsymbol{G} = \{ \boldsymbol{g}_m \}, \qquad (5)$$

where m – is the user access level, $m \in \{ 0, 1, \dots, M \}$.

There is a rigid hierarchy of subordination between privilege groups. Each group with a higher privilege level inherits from the group with the previous privilege level value. This makes it possible for high-privileged users to access sections with lower access privileges.

A set of system users is divided into disjoint subsets using access privilege groups, that is, a user can belong to only one access privilege group:

$$\bigcap_{m \in \left[0, M \right]} g_m = \emptyset, \qquad (6)$$

User access to sections of the network of portals is carried out in accordance with the access rules. Each such rule prescribes one of two possible actions: "allow" or "deny" user access to the section.

We denote the set of actions for user access to sections of the corporate portal network by $\boldsymbol{X}$. The elements of the set $\boldsymbol{X}$ are actions $\boldsymbol{x}_{wz}$:

$$\boldsymbol{X} = \{ \boldsymbol{x}_{wz} \}, \; w \in \boldsymbol{W}, \; z \in \boldsymbol{Z} \;. \qquad (7)$$

Each action of access $\boldsymbol{x}_{wz}$ of the user $\boldsymbol{u}_w$ to the section $\boldsymbol{q}_z$ takes the value $\boldsymbol{x}_{wz} = 1$ ("allow") or $\boldsymbol{x}_{wz} = 0$ ("deny"), depending on the values of the access levels of the user and the section of the corporate portal network. If the user's access level is greater than or equal to the section's access level, then in accordance with the rule, the user can access the section, otherwise, it is denied:

$$\boldsymbol{X} = \{ \boldsymbol{x}_{wz} \,|\, (\boldsymbol{m}_w \geq \boldsymbol{n}_z \Rightarrow \boldsymbol{x}_{wz} = 1), (\boldsymbol{m}_w < \boldsymbol{n}_z \Rightarrow \boldsymbol{x}_{wz} = 0) \}, \boldsymbol{m}_w, \boldsymbol{n}_z \in \{ 0, 1, \dots, M \}. \qquad (8)$$

In this case, the access rule begins to play the assigned role in the entire branch of the tree, which is formed by this object. For this, the system provides a mechanism for inheriting the access level of the parent object by child objects.

For each child section, the access level inheritance mechanism can be disabled, and a new access rule can be assigned, which will apply to it and all its descendants [6]. In the new rule, the access level for the section must be the same as that of the parent object, or higher than the access level of the parent object:

$$\boldsymbol{X}_b = \{ \boldsymbol{x}_{wb} \mid (\boldsymbol{m}_w \geq \boldsymbol{n}_b \Rightarrow \boldsymbol{x}_{wb} = 1), (\boldsymbol{m}_w < \boldsymbol{n}_b \Rightarrow \boldsymbol{x}_{wb} = 0) \}, \tag{9}$$
$$\boldsymbol{n}_b > \boldsymbol{n}_a , \boldsymbol{m}_w, \boldsymbol{n}_a \in \{ 0 , 1 , \dots , M \}.$$

where $\boldsymbol{X}_b$ – the set of user access actions to the $\boldsymbol{q}_b$ section; $\boldsymbol{x}_{wb}$ –the action for user $\boldsymbol{u}_w$ to access $\boldsymbol{q}_b$ partition.

It should be noted that each session of a user authorized in the system has a unique identifier that allows you to determine which user belongs to a request to the portal:

$$\boldsymbol{H} = \{\boldsymbol{h}_{wzt}\}, \; w \in \boldsymbol{W}, \; z \in \boldsymbol{Z}, \; t \in \boldsymbol{T}, \tag{10}$$

where $\boldsymbol{H}$ – set of sessions of using information resources of the corporate portal network; $\boldsymbol{h}_{wzt}$ – identifier of the user $\boldsymbol{u}_w$ access session to the information resources of the $\boldsymbol{P}_{6z}$ section at time t; $\boldsymbol{T}$ – set of values of points in time counted when taking into account requests for user access to sections of the corporate portal network.

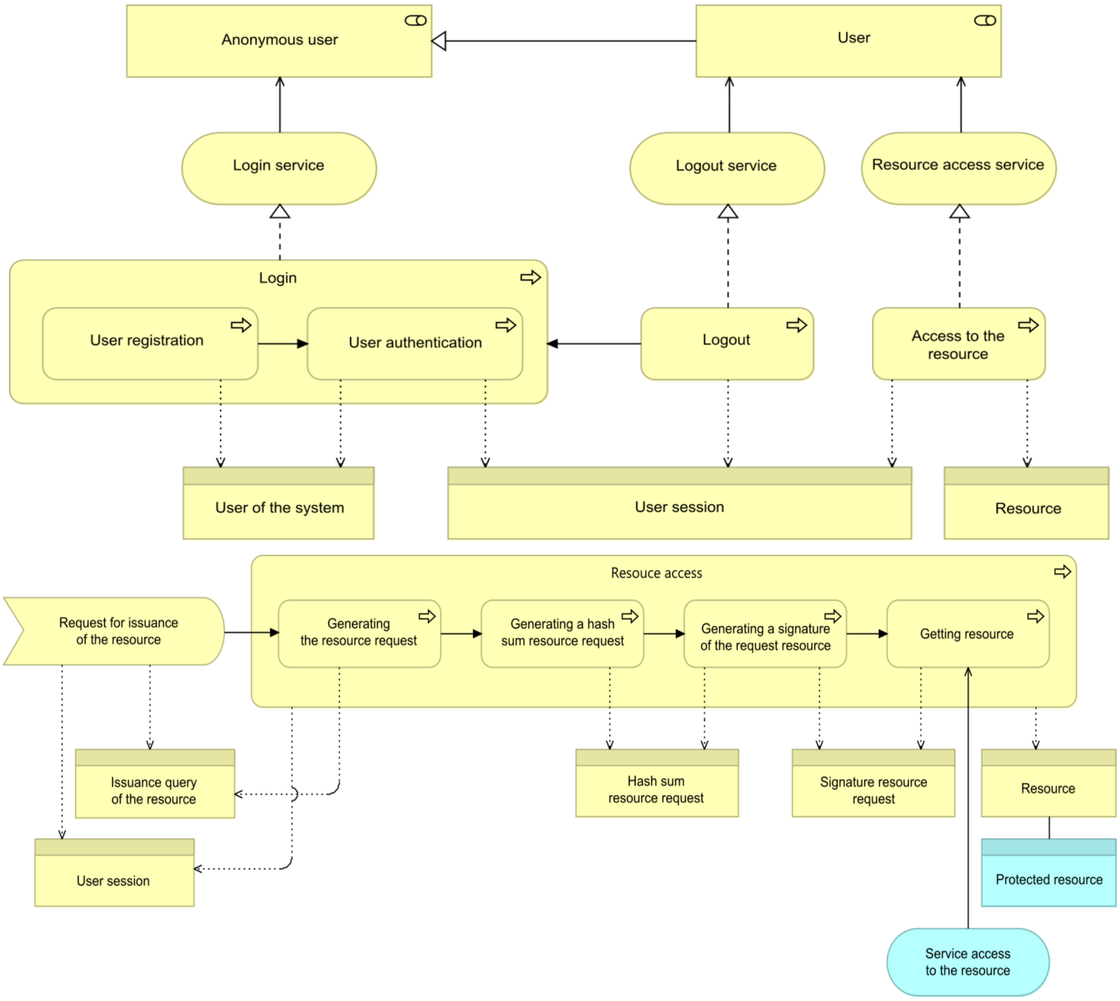
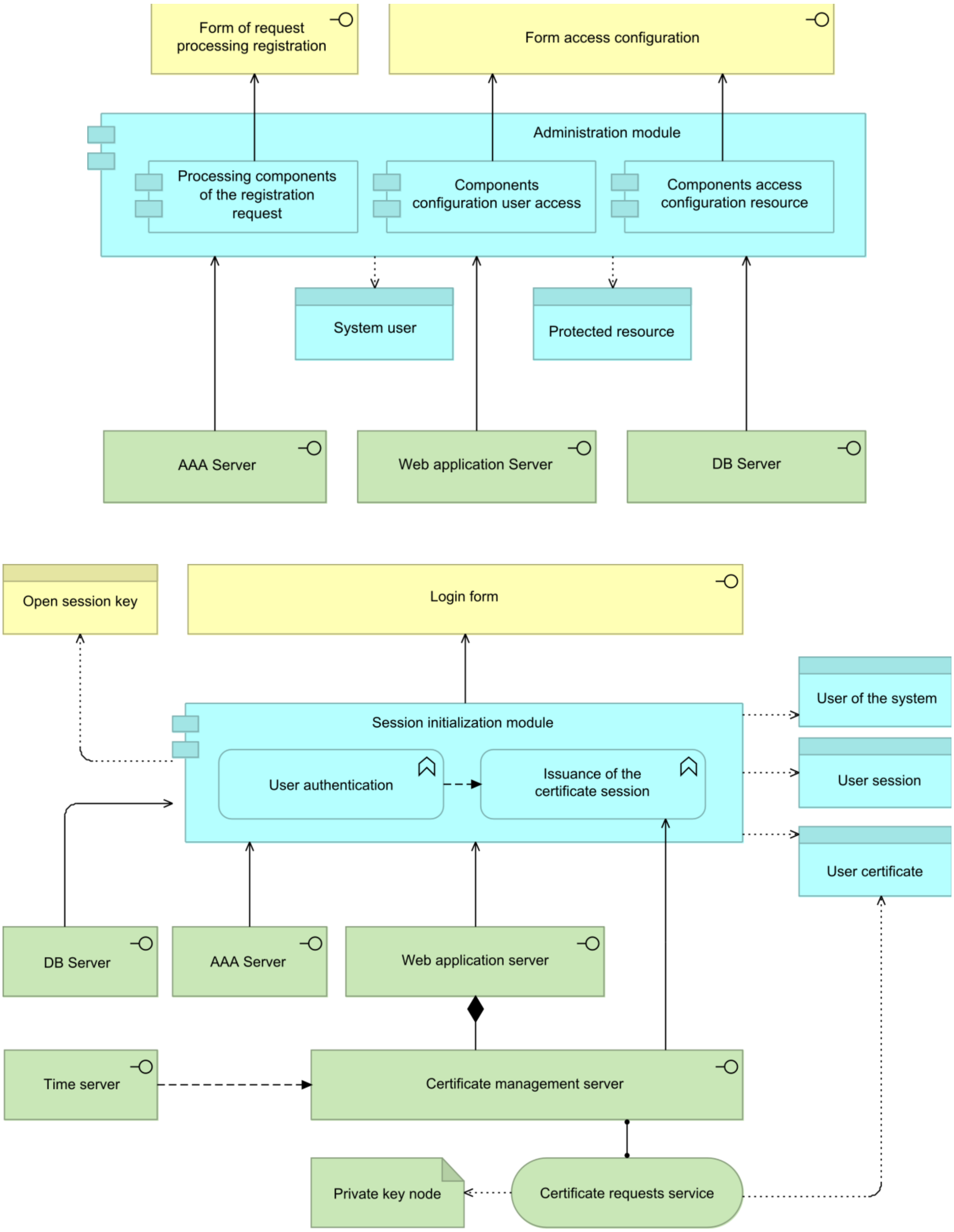

Anonymous user
User
Login service
Logout service
Resource access service
Login
User registration
User authentication
Logout
Access to the resource
User of the system
User session
Resource
Resouce access
Request for issuance of the resource
Generating the resource request
Generating a hash sum resource request
Generating a signature of the request resource
Getting resource
Issuance query of the resource
Hash sum resource request
Signature resource request
Resource
User session
Protected resource
Service access to the resource

Figure 2: Structure of presentation layer

The session identifier $\boldsymbol{h}_{wzt}$ in (10) is a concatenation of the values $\boldsymbol{P}_{9w1}$, $\boldsymbol{P}_{10,i,3}$, t , where i is the value of the counter of requests to the site at a relative time t:

$$h_{wzt} = \left(P_{9w1} \cdot 10^{1+int\left(\left(P_{10,\,i\,,\,3}\right)\right)} + P_{10,\,i\,,\,3}\right) \cdot 10^{1+int((t))} + t. \qquad (11)$$

The homomorphism of formula (11) can be used to execute the operator for concatenating the indexes of the section and the portal.



Form of request processing registration
Form access configuration
Administration module
Processing components of the registration request
Components configuration user access
Components access configuration resource
System user
Protected resource
AAA Server
Web application Server
DB Server
Open session key
Login form
Session initialization module
User authentication
Issuance of the certificate session
User of the system
User session
User certificate
DB Server
AAA Server
Web application server
Time server
Certificate management server
Private key node
Certificate requests service

Figure 3: Application layer structure

2.2.4. Implementing a secure virtual environment model

In a protected virtual environment, in relation to the applied task of organizing information exchange of scientific and educational organizations within the framework of the implementation of complex projects, three levels are distinguished:

- processes of information interaction, the basis for the implementation of which is a distributed database;
- infrastructure - a network of portals;
- information security, which is determined by the adopted policy.

The implementation of the described model of a protected virtual environment involves the construction of a distributed software package, which is divided into three layers:

- presentation layer;
- application layer (middle layer);
- data layer.

The presentation layer on Figure 2 provides interaction with the user and contains the components of the complex interface. Only the simplest program logic is brought to this level, which is responsible for displaying information and network interaction with the application layer.

The middle layer Figure 3 is represented by the application server, which contains the core program logic. Application servers are designed so that adding additional instances to them provides horizontal performance scaling of the software suite and does not require changes to the application program code.

The data layer includes source access components that encapsulate data storage mechanisms. This role is played by the data management application programming interface (API).

The organizational and structural diagram of a large scientific and educational consortium can reach significant sizes and include many branches. In this regard, an approach based on Binary Decision Diagrams (BDD) is used to implement access to protected information and computing resources.

Using BDD to represent data structures avoids linearizing the inheritance hierarchy.

BDD represents a Boolean function as a root acyclic graph. In BDD, nodes with the same function value are combined. If at each BDD level all vertices have the same label (the same variables), then such a BDD is called ordered or OBDD. OBDD vertices are arranged in levels, each level corresponds to one variable that marks the vertices located at this level. Binary decision diagrams are used as a compact form of Boolean function representation. This representation is useful in many cases when need to repeatedly calculate the values of a function for different sets of values of its arguments.

3. Conclusion

The authors obtained relationships for all elements of the tuples ***O***, ***P*** and their components.

The resulting model was used to build a secure virtual environment for scientific and educational organizations as an authentication algorithm and control user access to portal resources. In the full version of the model of a protected virtual environment for the administration of information exchange of scientific and educational organizations, the authors considered a model of a network of corporate portals and an assessment of the effectiveness of managing information exchange in this network based on probabilistic indicators. This made it possible to assess the performance of the project of the developed software and hardware solutions for the virtual environment for the administration of information exchange of scientific and educational organizations.

4. References

[1] S. Leng, Algebra, In Russian, Moscow, 1968.

[2] N. K. Vereshchagin, and A. Shen, Lectures on mathematical logic and theory of algorithms, In Russian, Moscow, 2012.

[3] S. A. Lazarev, and A.V. Demidov, The Concept of Construction of a Control System of an Information Exchange in The Network of Corporate Portals, Information Systems and

Technologies, 2010, no. 4(60), pp. 123–129. URL: http://oreluniver.ru/public/file/archive/isit%204-2010.pdf.

[4] S. A. Lazarev, I. S. Konstantinov, and O.V. Mihalev, Realization of a single model session access in the distributed network portals, Vestnik komp'iuternykh i informatsionnykh tekhnologii (Herald of computer and information technologies), 2014, no. 6, pp. 44–49. doi: 10.14489/vkit.2014.06.pp.044-049.

[5] K. Hrbacek, T. Jech, Introduction to Set Theory, Third edition, revised and expanded, 1999.

[6] T. Takagi, and M. Sugeno, Fuzzy identification of systems and its applications to modeling and control, IEEE Transactions on Systems, Man, and Cybernetics, vol. 15, no 1, 1985, pp. 116–132. doi:10.1109/TSMC.1985.6313399.

[7] H. Blaine, The Threat Landscape of PKI: System and Cryptographic Security of X.509, Algorithms, and their Implementations, Proceedings of the Romanian Academy, Series A, vol. 14, 2013, pp. 286–294. URL: https://academiaromana.ro/sectii2002/proceedings/doc2013-3s/02-HEIN.pdf.

[8] M. Benantar, Access control systems: Security, identity management and trust models, Springer US, 2006. doi:10.1007/0-387-27716-1.

[9] S.-K. Chin, Access control, security, and trust: A logical approach, CRC Press, 2010. doi: 10.1201/9781439894637.

[10] K.-C. Li, X. Chen and W. Susilo, Advances in cyber security: Principles, techniques, and applications, Springer Singapore, 2018. doi: 10.1007/978-981-13-1483-4.

[11] E. Al-Shaer, X. Ou and G. Xie, Automated security management, Springer International Publishing, 2013. doi: 10.1007/978-3-319-01433-3.

[12] A. Sadiqui, Computer network security, Wiley, 2020. doi: 10.1002/9781119706762.

[13] K. Al-Begain, M. Zak, W. Alosaimi and C. Turyagyenda, Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, IGI Global, 2018. doi: 10.4018/978-1-5225-5634-3.

[14] R. Matulevičius, Fundamentals of secure system modelling, Springer International Publishing, 2017. doi: 10.1007/978-3-319-61717-6.

[15] A. Wong and A. Yeung, Network infrastructure security, Springer US, 2009. doi: 10.1007/978-1-4419-0166-8.