УДК 519.724 +004.722

Сергей.А ЛАЗАРЕВ, Конст.А РУБЦОВ
Sergey.A. LAZAREV, Konst.A. RUBTSOV

О МОДЕЛИ ЗАЩИЩЕННОЙ ВИРТУАЛЬНОЙ СРЕДЫ НАУЧНО-ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ
ABOUT THE PROTECTED VIRTUAL ENVIRONMENT MODEL SCIENTIFIC AND EDUCATIONAL ORGANIZATIONS

В данной работе авторы освещают вопросы построения теоретико-множественной модели защищенной виртуальной среды информационного взаимодействия научно-образовательных организаций, на основе описания отношений сущностей и правил информационного обмена. Предлагается способ описания состава, структуры классов и их иерархия, позволяющих представить с помощью теории множеств и исчисления предикатов объектную модель организационно-технического объединения субъектов информационного взаимодействия в рамках единой модели управления и политики безопасности. Разработана модель сеансового к информационным ресурсам сети корпоративных порталов.

Ключевые слова: защищенная виртуальная среда, модель объектной системы, описание объектных моделей.

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

Keywords: secure virtual environment, object system model, description of object models.

Защищенная виртуальная среда информационного взаимодействия отображается в информационном пространстве организационно-технического объединения субъектов информационного взаимодействия в рамках ассоциаций, консорциумов или сетевых структур для реализации совместных проектов и решения общих задач. В качестве субъектов информационного взаимодействия в рамках ассоциаций, консорциумов или сетевых структур выступают регулирующие органы, внешние субъекты, члены объединения и их подразделения, сотрудники, а также определенная для каждого субъекта политика безопасности. Для реальных (физических) субъектов информационного взаимодействия могут быть выделены основные сущности описывающих их характеристики как множество субъектов O. Это множество отображается на множество P, которое является множеством виртуальных объектов, существующих только в рамках защищенной среды. Таким образом, защищенная виртуальная среда обеспечивает интеграцию разнородных распределенных информационно-вычислительных ресурсов принадлежащим различным субъектам, под контролем единого координирующего центра, реализующего функции защищенного информационного взаимодействия в рамках единой модели управления и политики безопасности. Защищенная виртуальная среда строится на основе существующей

программно-аппаратной инфраструктуры используя публичные порталы и каналы связи, то есть является полностью виртуальной структурой информационного взаимодействия.

В настоящее время доминирующей методологией, используемой при разработке приложений и информационных систем, является объектно-ориентированный подход. В данной работе авторы рассматривают модель отношения сущностей при описании виртуальной среды информационного взаимодействия научно-образовательных организаций. Основным звеном взаимодействия является портал, который рассматривается как совокупность взаимосвязанных разделов (объектов доступа), имеющих иерархическую древовидную структуру подчиненности. Для каждого раздела портала может быть назначено только одно правило доступа, распространяющееся на всю ветвь дерева объектов за счет механизма наследования дочерними объектами прав доступа родительского объекта. Для дочернего объекта может быть отключен механизм наследования прав и назначены новые правила доступа, которые будут наследованы его потомками. В качестве математического аппарата описания теоретико-множественной модели защищенной виртуальной среды информационного взаимодействия научно-образовательных организаций используется теория множеств и математическая логика [1-2].

Пусть $\overline{p}$ вектор, состоящий из множеств объектов портала P, а $\overline{o}$ вектор из множеств субъектов и сущностей информационного взаимодействия в рамках ассоциаций, консорциумов или сетевых структур научно-образовательных организаций. Защищенная виртуальная среда их взаимодействия является множеством $S = \left\{\overline{o}, \overline{p}\right\}$, при этом множество объектов вектора $\overline{o}$ является инъекцией в P: $O \to P$.

Авторы выделили основные элементы векторов $\overline{o}$ и $\overline{p}$: $\overline{o} = \left\langle \overline{o_i} \right\rangle$, $i = \overline{1,7}$; $\overline{p} = \left\langle \overline{p_j} \right\rangle$, $j = \overline{1,10}$, где $\overline{o_1}$ –регулирующие органы, $\overline{o_2}$ –внешние субъекты, $\overline{o_3}$ –объединения, $\overline{o_4}$ – участники объединения, $\overline{o_5}$ –подразделения объединения, $\overline{o_6}$ –сотрудники подразделения объединения, $\overline{o_7}$ –политика безопасности объединения, $\overline{p_1}$ –учреждение, $\overline{p_2}$ –сервер управления, $\overline{p_3}$ –сервер доступа, $\overline{p_4}$ –пользовательский домен, $\overline{p_5}$ –ресурс портала, $\overline{p_6}$ – разделы доступа, $\overline{p_7}$ –группа уровней доступа, $\overline{p_8}$ –права доступа, $\overline{p_9}$ –учетная запись, $\overline{p_{10}}$ – запрос к сайту. Соответственно множества, соответствующие указанным векторам, обозначим как $O = \left\{O_i\right\}$, $i = \overline{1,7}$; $P = \left\{P_j\right\}$, $j = \overline{1,10}$.

Элементы векторов $\overline{o}$ и $\overline{p}$, фактически, являются множествами с описанием их структурных элементов и методов их информационного взаимодействия. Однако, структурные элементы, в основном, это вектора, состоящие из векторов или множеств типизированных данных. Например, для $\overline{o_4} = \left\langle \overline{o_{4i}} \right\rangle$, $i = \overline{1,5}$, где $\overline{o_{41}}$– вектор с наименованиями членов объединения, $\overline{o_{42}}$ – вектор с идентификатором члена объединения, $\overline{o_{43}}$ –вектор с юридическим адресом, $\overline{o_{44}}$ – вектор с банковскими реквизитами, $\overline{o_{45}}$ – вектор с ролью участника объединения.

При выполнении сеансовых запросов аутентификацией [3, 4] в портале формально можно определить как вектор $\overline{p} = \left\langle A, C, D \right\rangle$, где $A = \left\{a_i\right\}$ –множество узлов контроля

доступа $A \in P_3$ $i = \overline{1, n}$; $C = \{c_j\}$ –множество узлов управления сетью $C \in P_2$, $j = \overline{1, m}$; $D = \{d_i\}$ –множество пользовательских доменов в сети $D \in P_4$. Под пользовательским доменом подразумевается уникально именованная группа пользователей, которая представлена кортежем: $d_i = \langle U_i, D_i' \rangle$, где U_i –множество пользователей *i*-го домена, $i = \overline{1, n}$, D_i' –подмножество доменов в сети с доверительными отношениями домена d_i, $D_i' \subseteq D$ и $d_i \in D_i'$. Каждый пользовательский домен соответствует конкретному узлу контроля доступа сети и наоборот, $A \leftrightarrow D$. В каждом пользовательском домене d_i существует подмножество авторизированных в данный момент времени пользователей $U_i' \subset U_i$. Узел управления сетью представляет собой кортеж $c_i = \langle S^0, R^0, D \rangle$, где S^0 – множество всех активных пользовательских сеансов сети порталов; R^0 –множество всех идентифицированных запросов в сети. Узел контроля доступом можно представить как кортеж: $a_i = \langle S_i, R_i, D_i' \rangle$, где S_i –множество активных пользователей сеансов узла контроля доступа, R_i –множество идентифицированных запросов к узлу контроля доступа. Модель сеансового доступа:

$$\forall a_i : \exists s_{ik} \in S_i, u_{qz}' \in U_q', d_q \in D_i' \Rightarrow T : s_{ik} \to u_{qz}', \quad (1)$$

где a_i –узел контроля доступа, u_{qz}' – *z*-й авторизированный пользователь сеанса s_{ik} домена d_q, $q = \overline{1, n}$, T –функция соответствия пользователя и его сеанса.

Запрос пользователя защищенной виртуальной среды информационного взаимодействия считается идентифицированным, когда возможно определить его инициатора на основе условия (1) по активному сеансу:

$$\forall r_{ikx} \in R_i : \exists s_{ik} \in S_i \Rightarrow E : r_{ikx} \to s_{ik}, \quad (2)$$

где r_{ikx} –запрос *x* к *i*-му узлу, содержащий метку *k* пользовательского сеанса, E –функция идентификации пользовательского сеанса по запросу, а отношение F_A определяющее разрешение доступа пользователя к ресурсу: $\exists F_A : U \times R \to \{true, false\}$.

Таким образом, для идентификации пользовательского сеанса (2) необходимо и достаточно наличие сеансовых данных только на узле контроля доступа, обрабатывающего запрос.

Следует отметить, что каждый сеанс авторизованного в системе пользователя имеет уникальный идентификатор, позволяющий определить, какому пользователю принадлежит тот или иной запрос к порталу:

$$H = \{h_{wzt}\}, \ w \in W, \ z \in Z, \ t \in T, \quad (3)$$

где H – множество сеансов использования информационных ресурсов сети корпоративных порталов; h_{wzt} – идентификатор сеанса доступа пользователя u_w к информационным ресурсам раздела P_{6z} в момент времени t; T – множество значений моментов времени, отсчитываемых при учете запросов доступа пользователей к разделам сети корпоративных порталов.

Идентификатор сеанса h_{wzt} в (3) является конкатенацией значений $P_{9w1}, P_{10,i,3}, t$, где i –значение счетчика запросов к сайту в относительный момент времени t:

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

Авторами получены взаимосвязи, для всех элементов векторов $\bar{o}$ и $\bar{p}$ и их компонентов.

Полученная модель был применена для построения защищенной виртуальной среды научно-образовательных организаций в качестве алгоритма аутентификации и контроля доступа пользователей к ресурсам портала.

СПИСОК ЛИТЕРАТУРЫ

1. Lazarev S.A., Demidov A.V. 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.

2. Lazarev S.A., Konstantinov I.S., Mihalev O.V. 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.

3. Takagi T., Sugeno M. 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.

4. Blaine H. 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.

Лазарев Сергей Александрович

Белгородский государственный национальный исследовательский университет, г. Белгород

К.э.н., заведующий лабораторией прикладного системного анализа и информационных технологий

Тел.: +7-915-527-36-65

E-mail: lazarev_s@bsu.edu.ru

Рубцов Константин Анатольевич

Белгородский государственный национальный исследовательский университет, г. Белгород

К.т.н., заведующий учебно-научной лаборатории информационно-измерительных и управляющих комплексов и систем

Тел.: +7-904-088-08-48

E-mail: rubtsov@bsu.edu.ru