

Архитектура комбинированной системы э-обучения: модельное исследование процессов защиты информационных ресурсов ¹

Романски Ради Петров
профессор, д.т.н. инж., кафедра Информатики,
Технический Университет - София,
ул. Кл. Охридского, 8, г. София - 1000, Болгария
rrom@tu-sofia.bg

Нонинска Ирина Станчева
доцент, д-р инж., кафедра Компьютерных систем,
Технический Университет - София,
ул. Кл. Охридского, 8, г. София - 1000, Болгария
irno@tu-sofia.bg

Аннотация

Цель статьи - представить результат исследований процессов защиты информационных ресурсов комбинированной системы э-обучения, включающей два типа ресурсов – внутренних (сохраняемых в собственной памяти) и внешних (сохраняемых в облачных центрах данных и используемых посредством облачных услуг). Представлена основная архитектурная концепция системы и предложена формализация процессов. Исследование реализовано с помощью аппарата сетей Петри, при этом использовано расширение на основе модели Маркова, чтобы отобразить стохастический характер процессов. Представлены также статистические оценки основных параметров.

The goal is to present some results from an investigation of the processes for secure access to the information resources in a combined e-learning system. The system is based on two types resources – internal (stored in own memory units) and external (stored in a cloud data centre and used by cloud services). The architecture of the system is presented and a formal description is proposed. The investigation is realised by using the Petri net apparatus and an extension based on Markov's processes for presentation the stochastic nature of the processes is proposed. Some statistical assessments for the basic parameters are given.

Ключевые слова

комбинированная среда э-обучения, защита информации, облачные услуги, моделирование, статистические оценки
combined e-learning environment, information security, cloud services, modelling, statistical assessments

Введение

Электронное обучение развивается непрерывно: постоянно предлагаются различные новые методы, модели и технологии э-обучения. Например, в [1]

¹ Работа выполнена при поддержке гранта НФНИ – МОН № ДН07/10-2016, Болгария.

предлагается новый подход к виртуальному обучению „... который интегрирует в себя особенности уже существующих, открывает новые горизонты и возможности в получении определенных навыков и умений.“. Авторы указывают на то, что „новый подход заключается во внедрении в типовую архитектуру системы электронного обучения новой составляющей ...“, которая на основе современных информационных технологий (ИТ) позволит достичь „... улучшения качества и повышения эффективности обучения и образовательного процесса в целом“.

Электронное образование (э-образование) является основной частью современного информационного общества (ИО) и многие из инициатив Европейской комиссии (ЕК) связаны с развитием таких систем. За последние несколько лет в цифровом пространстве усиленно вводятся технологии облачных услуг [2] и социальные коммуникации [3]. В таком аспекте в [4] подчеркивается, что „использование технологии облачных вычислений является неотъемлемой составляющей современного технического образования...“ и в дополнение указывается, что „... облачные вычисления подразумевают хранение и доступ к данным и программам через Интернет вместо жесткого диска вашего компьютера.“. Рогальский [5] отмечает „Есть еще одна причина, требующая ускорения наших разработок в этой области. Это повсеместный переход на облачные вычисления.“

Современные системы э-образования используют сетевые возможности цифрового мира, используя виртуальную реальность, форумы, социальные медиа, облачные услуги и др. при реализации различных форм, как например, электронная (e-learning), дистанционная или распределенная (d-learning), мобильная (m-learning) [6] и др. Результатом является разработка новых архитектурных решений, например, базированных на облачных услугах [7], или на новых моделях, как, например, предлагается в [8] (“collaborative learning”). Цель этой модели – отреагировать на ситуацию со все более возрастающим числом обучаемых при относительно уменьшающемся числе университетских преподавателей. Все эти новые технологии требуют применения новых и адекватных мер при защите данных в облачном пространстве [9] и в особенности потребительских профилей, содержащих личные данные [10].

Другой аспект применения облачных технологий представлен в [11], где авторы предлагают экспертную консультантскую систему определения наилучшей облачной модели для э-образовательной системы. В [12] предлагается подход в подборе партнеров при создании „облачного“ консорциума, основанного на моделировании при помощи теории цепей Маркова (процесс Маркова с дискретными состояниями и непрерывным временем переходов).

Цель статьи - представить модельное исследование процессов по защите информационных ресурсов в системе э-образования, основанной на комбинировании традиционного подхода с возможностями облачных технологий. Архитектура такой системы описана в [13]. Основной проблемой является то, что отдаленный множественный доступ к такой системе требует применения процедур по защите информационных ресурсов (образовательных материалов, системных файлов, профилей и интересов, образовательного статуса, персональных данных, журнальных файлов и т.п.), как и внедрения Системы управления правами доступа (DRMS – Digital Rights Management System). Модельное исследование проведено на основе предварительной формализации процессов и разработки аналитических моделей при помощи теории цепей Петри и Марковских процессов.

Архитектура комбинированной системы э-образования и защита данных

Облачные услуги имеют множество преимуществ, но они четко ставят также и вопросы информационной безопасности сетевых систем и, главным образом, защиты персональных данных. Право на личную жизнь (privacy) является всепризнанным человеческим правом, оно должно быть обеспечено в современном цифровом мире [14]. Как правило, политика защиты личных данных должна рассматриваться в контексте политики по защите информационных ресурсов при соблюдении национального и Европейского законодательства. Это имеет существенное значение в использовании облачных услуг и разработке архитектур, использующих облако и, как отмечается в [15], „безопасность облачной информационной системы в значительной степени взаимосвязана с ее архитектурой и атрибутами“. В этом направлении рекомендуется осуществление предварительного исследования, как это сделано в [16], где проведен „анализ стохастических методов, используемых для моделирования поведения и оценки показателей готовности, надежности облачных инфраструктур“. В статье указаны в качестве подходящих методы исследования „1) моделирование на основе использования сетей Петри; 2) моделирование на основе использования марковских цепей“, при этом „в случае нарушения свойства марковости ... предлагается применять аппарат моделирования полумарковских процессов...“.

На рисунке 1 представлена концептуальная модель организации комбинированной системы электронного образования [13], в которой указаны основные участники (преподаватель и студент) и определены две основные компоненты – внутренняя среда и внешние объекты (интернет, облако, социальные медиа, сайты). Концепция развита в архитектуре системы, представленной на рисунке 2.



Рис. 1. Концептуальная модель организации комбинированной системы э-образования [13]

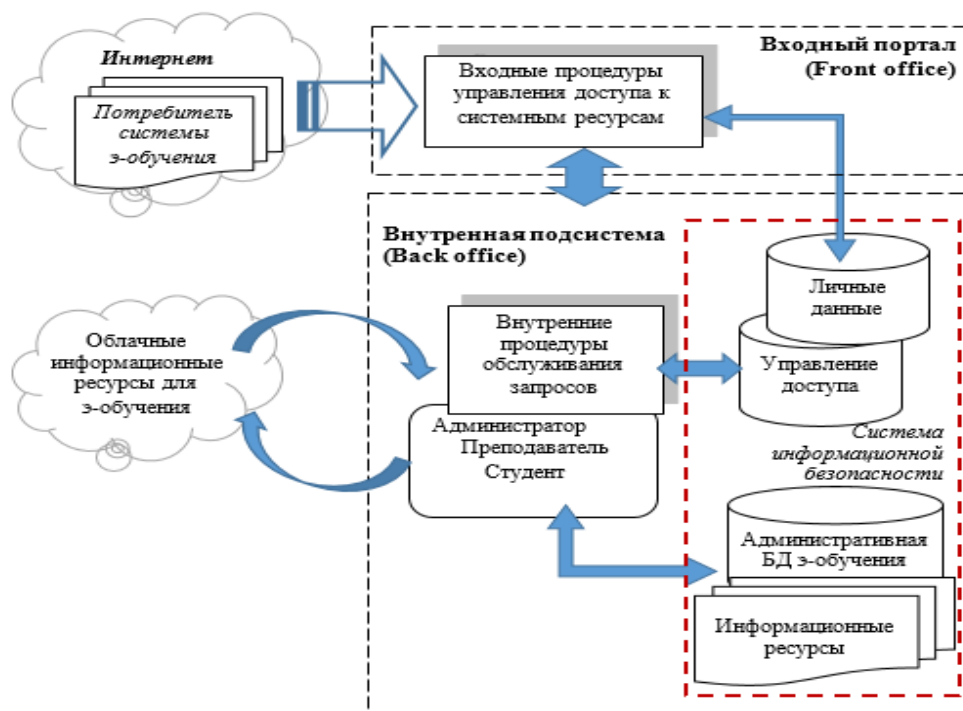


Рис. 2. Архитектура комбинированной системы для э-образования

Архитектура включает следующие основные компоненты:

- ♦ **Входной портал (Front office)** – входная точка отдаленного доступа к системе для внешних пользователей, обеспечивающая управление доступом при помощи идентификации, регистрации и аутентификации. Идентификация должна обеспечить опознаваемость пользователя, осуществившего доступ. При регистрации открывается профиль нового пользователя, собирая при этом только самые необходимые для этой цели данные. Аутентификация обеспечивает легитимность доступа к системным и информационным ресурсам среды. Дополнительной функцией является поддержка журнального файла для каждого доступа (время, IP адрес и другие существенные атрибуты доступа).

- ♦ **Внутренняя подсистема административного обслуживания поступивших запросов (Back office)**, которая обслуживает поступившие легитимные запросы на основе определения права доступа (аутентификация). В ее структуре находится система информационной безопасности, объединяющей процедуры и технологические средства защиты ресурсов и доступа к персональным профилям. Основные функции поддерживаются Digital Rights Management System (DRMS).

- ♦ **Наборы информационных и образовательных ресурсов** поддержки процессов э-образования, распределенные как внутренние (сохраняемые в собственной памяти) и внешние (сохраняемые в облачных центрах данных, включая социальные медиа и сети, сайты и т.пр.).

Формализация процессов поддержки легитимного и защищенного доступа к системным и информационным ресурсам показана на рисунке 3. Основные процедуры выполняют задачи аутентификации и авторизации доступа, а также регламентирования сбора, актуализации, сохранения и обработки личных данных, включая их архивирование и уничтожение по истечении необходимости в их поддержке.



Рис. 3. Формализация процессов для защиты информационных ресурсов

Реализация детерминированной модели и дерево достижимости

Детерминированная модель, реализованная с использованием теории сети Петри, представлена ниже в виде теоретико-множественного определения $PN = \{T, P, I, O\}$, где $T \cap P = \emptyset$.

Множество переходов $T = \{t_i / i=1 \div 8\}$ в PN-модели:

- t_1 – процедура идентификации поступившего запроса;
- t_2 – процедура регистрации нового пользователя;
- t_3 – процедура аутентификации (authentication) – опознавание идентифицированного (легитимного) пользователя;
- t_4 – выход из системы по причине нелегитимного доступа или отказа от обслуживания;
- t_5 – анализ легитимного запроса доступа информационного/системного ресурса;
- t_6 – процедура авторизации (authorization) – проверки полномочий доступа и использования внешних ресурсов, сохраненных в облачном центре данных;
- t_7 – процедура авторизации (authorization) – проверки полномочий доступа и использования внутренних ресурсов, сохраненных в собственных запоминающих устройствах;

t_8 – конец обслуживания по текущему запросу и анализ последующих действий.

Процедуры t_6 и t_7 используют „Системы управления доступом“ (DRMS – Digital Right Management Systems).

Множество позиций $P = \{p_j / j=1 \div 7\}$ в PN-модели:

p_1 – наличие запроса доступа к системе (вход с внешнего источника к portalу системы);

p_2 – запрос от незарегистрированного источника (пользователя);

p_3 – запрос от зарегистрированного источника (пользователя);

p_4 – наличие результата после проведенной аутентификации (опознавание пользователя), при этом результатом является „легитимный доступ“ или „нелегитимный доступ“;

p_5 – анализированный запрос доступа к внешнему ресурсу в облаке;

p_6 – анализированный запрос доступа к внутреннему ресурсу в системе;

p_7 – наличие обслуженного запроса для определения последующих действий.

Входные функции:

$I(t_1) = \{p_1\}$

$I(t_2) = \{p_2\}$

$I(t_3) = \{p_3, p_3\}$

$I(t_4) = \{p_4\}$

$I(t_5) = \{p_4\}$

$I(t_6) = I(t_7) = \{p_5, p_6\}$

$I(t_8) = \{p_7\}$

Выходные функции:

$O(t_1) = \{p_2, p_3\}$

$O(t_2) = \{p_3\}$

$O(t_3) = \{p_4\}$

$O(t_4) = \{p_1\}$

$O(t_5) = \{p_5, p_6\}$

$O(t_6) = O(t_7) = \{p_7\}$

$O(t_8) = \{p_4\}$

Граф-схема предложенной модели представлена на рисунке 4.

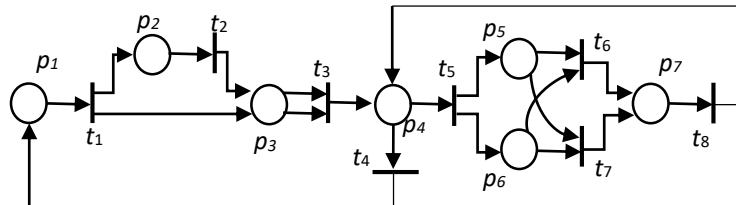


Рис. 4. Граф-схема детерминированной PN-модели

Решение модели (эволюция сети Петри) представлено на рисунке 5 при помощи дерева достижимости от последовательных маркировок на основе разрешенных переходов. В таблице 1 прослеживается эволюция сети в последовательных шагах.

$$\begin{aligned}
 \mu_0 &= (1,0,0,0,0,0,0) \xrightarrow{t_1} \mu_1 = (0,1,1,0,0,0,0) \xrightarrow{t_2} \mu_2 = (0,0,2,0,0,0,0) \\
 \mu_2 &\xrightarrow{t_3} \mu_3 = (0,0,0,1,0,0,0) \\
 \mu_3 &\xrightarrow{t_4} (1,0,0,0,0,0,0) \equiv \mu_0 \\
 \mu_3 &\xrightarrow{t_5} \mu_4 = (0,0,0,0,1,1,0) \\
 \mu_4 &\xrightarrow{t_6} \mu_{51} = (0,0,0,0,0,0,1) \xrightarrow{t_8} (0,0,0,1,0,0,0) \equiv \mu_3 \\
 \mu_3 &\xrightarrow{t_7} \mu_{52} = (0,0,0,0,0,0,1) \xrightarrow{t_8} (0,0,0,1,0,0,0) \equiv \mu_3
 \end{aligned}$$

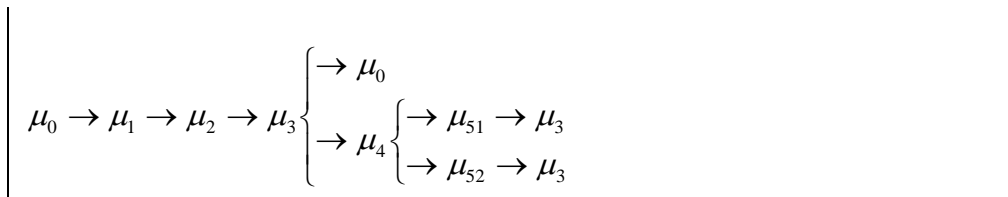


Рис. 5. Дерево достижимости эволюции PN-модели

Таблица 1.

Эволюция PN-модели

$\mu_{\text{текущая}}$	Разрешенный переход	Активный переход	$\mu_{\text{новая}}$	Число марок в позициях						
				$p1$	$p2$	$p3$	$p4$	$p5$	$p6$	$p7$
μ_0	t_1	t_1	μ_1	1	0	0	0	0	0	0
μ_1	t_2	t_2	μ_2	0	1	1	0	0	0	0
μ_2	t_3	t_3	μ_3	0	0	2	0	0	0	0
μ_3	$t_4 \& t_5$	t_4	μ_0	0	0	0	1	0	0	0
		t_5	μ_4	0	0	0	0	1	1	0
μ_4	$t_6 \& t_7$	t_6	μ_{51}	0	0	0	0	0	0	1
		t_7	μ_{52}	0	0	0	0	0	0	1
μ_{51}	t_8	t_8	μ_3	0	0	0	1	0	0	0
μ_{52}	t_8	t_8	μ_3	0	0	0	1	0	0	0

Стохастическая версия модели и аналитическое решение

Дополнительное модельное исследование дискутируемых процессов в комбинированной среде э-обучения можно провести посредством применения расширенных версий сетей Петри (PN). Классический аппарат PN является дискретной структурой, которая может быть дополнена с учетом опоздания при осуществлении переходов $\theta_i = \theta(t_i)$, как это происходит во временных сетях Петри (Timed PN – TPN), в которых основным определением является $TPN := (P, T, I, O, \Theta)$, где $\Theta = \{\theta_1, \theta_2, \dots, \theta_n\}$. Для отражения вероятностной природы процессов в средах информационной обработки можно применить аппарат стохастических сетей Петри (Stochastic PN – SPN), при котором формальное определение представляет собой упорядоченную структуру $SPN := (P, T, I, O, L)$ с множеством $L = \{\lambda_1, \dots, \lambda_n\}$ интенсивностей каждого из переходов $\lambda_i = 1/\theta_i$. Такой подход использован в [17] при исследовании доступа к информационным ресурсам в глобальном пространстве.

Далее представлен модифицированный подход при рассмотрении эволюции представленной PN-модели при помощи Марковского процесса с дискретными состояниями $S = \{s_1, \dots, s_n\}$, соответствующими определенным маркировкам ($s_i \equiv \mu_i$), с вероятностными переходами между ними. Это позволяет определить аналитическую стохастическую модель в качестве цепи Маркова и исследовать условия стационарного режима.

а) компоненты Марковской модели:

✓ множество состояний

$$S = \{s_0 \leftrightarrow \mu_0, s_1 \leftrightarrow \mu_1, s_2 \leftrightarrow \mu_2, s_3 \leftrightarrow \mu_3, s_4 \leftrightarrow \mu_4, s_5 \leftrightarrow \mu_{51}, s_6 \leftrightarrow \mu_{52}\}; |S|=7$$

✓ вектор начальных состояний

$$P_0 = \{1, 0, 0, 0, 0, 0, 0\}$$

✓ матрица переходных вероятностей

$$P_{ij} =$$

	s_0	s_1	s_2	s_3	s_4	s_5	s_6
s_0	0	1	0	0	0	0	0
s_1	0	0	1	0	0	0	0
s_2	0	0	0	1	0	0	0
s_3	a	0	0	0	$1-a$	0	0
s_4	0	0	0	0	0	b	$1-b$
s_5	0	0	0	1	0	0	0
s_6	0	0	0	1	0	0	0

б) аналитическая модель:

✓ граф состояний марковской модели (рис. 6)

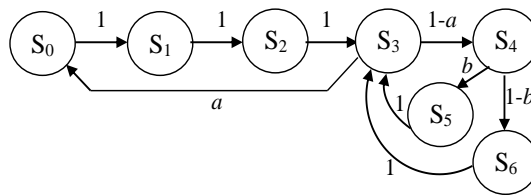


Рис. 6. Граф состояний марковской цепи

✓ аналитическое определение модели

$$(1): p_0 = a \cdot p_3$$

$$(2): p_1 = p_0$$

$$(3): p_2 = p_1$$

$$(4): p_3 = p_2 + p_5 + p_6$$

$$(5): p_4 = (1-a) \cdot p_3$$

$$(6): p_5 = b \cdot p_4$$

$$(7): p_6 = (1-b) \cdot p_4$$

$$(8): \sum_{j=0}^6 p_j = 1$$

в) аналитическое решение модели:

$$p_1 = p_2 = p_0$$

$$p_0 = a \cdot p_3 \Rightarrow p_3 = \frac{1}{a} \cdot p_0$$

$$p_4 = (1-a) \cdot p_3 = (1-a) \cdot \left(\frac{1}{a} \cdot p_0 \right) = \frac{1-a}{a} \cdot p_0$$

$$p_5 = b \cdot \left(\frac{1-a}{a} \cdot p_0 \right) = \frac{b \cdot (1-a)}{a} \cdot p_0$$

$$p_6 = (1-b) \cdot \left(\frac{1-a}{a} \cdot p_0 \right) = \frac{(1-a) \cdot (1-b)}{a} \cdot p_0$$

$$\begin{aligned}
\sum_{j=0}^6 p_j &= 1 \Rightarrow 3 \cdot p_0 + \frac{1}{a} \cdot p_0 + \frac{1-a}{a} \cdot p_0 + \frac{b-ab}{a} \cdot p_0 + \frac{1-a-b+ab}{a} \cdot p_0 = 1 \\
p_0 \left(3 + \frac{1}{a} + \frac{1-a}{a} + \frac{b-ab}{a} + \frac{1-a-b+ab}{a} \right) &= 1 \\
p_0 \cdot \frac{1}{a} \cdot (3a + 1 + 1 - a + b - ab + 1 - b - a + ab) &= 1 \Rightarrow p_0 = \frac{a}{a+3} = p_1 = p_2 \\
p_4 &= \frac{1-a}{a} \cdot p_0 = \frac{1-a}{a} \cdot \frac{a}{a+3} = \frac{1-a}{a+3} \\
p_5 &= \frac{b \cdot (1-a)}{a} \cdot \frac{a}{a+3} = \frac{b \cdot (1-a)}{a+3}; \quad p_6 = \frac{(1-b) \cdot (1-a)}{a} \cdot \frac{a}{a+3} = \frac{(1-b) \cdot (1-a)}{a+3}
\end{aligned}$$

г) аналитические выражения финальных вероятностей при стационарном режиме:

$$p_0 = p_1 = p_2 = \frac{a}{a+3}; \quad p_4 = \frac{1-a}{a+3}; \quad p_5 = \frac{b \cdot (1-a)}{a+3}; \quad p_6 = \frac{(1-b) \cdot (1-a)}{a+3}$$

д) статистические оценки:

В целях исследования определено множество выбранных стоимостей управляемых параметров a и b . При этом учитывалась функциональность и ответственность соответствующих процедур и ожидаемая средне-статистическая оценка реализации переходов между соответствующими состояниями (от S_3 и S_4 к следующим). Для параметра a определено множество стоимостей $\{0,1; 0,2; 0,3; 0,4; 0,5; 0,6; 0,7; 0,8; 0,9; 1\}$, а для параметра b – диапазон изменения от 0,3 до 0,7 при шаге $\Delta=0,1$. Применяется полный факторный план определенных множеств уровней параметров a и b . На рисунке 7 представлена графическая интерпретация обобщенных экспериментальных результатов среднестатистических оценок финальных вероятностей при стационарном режиме.

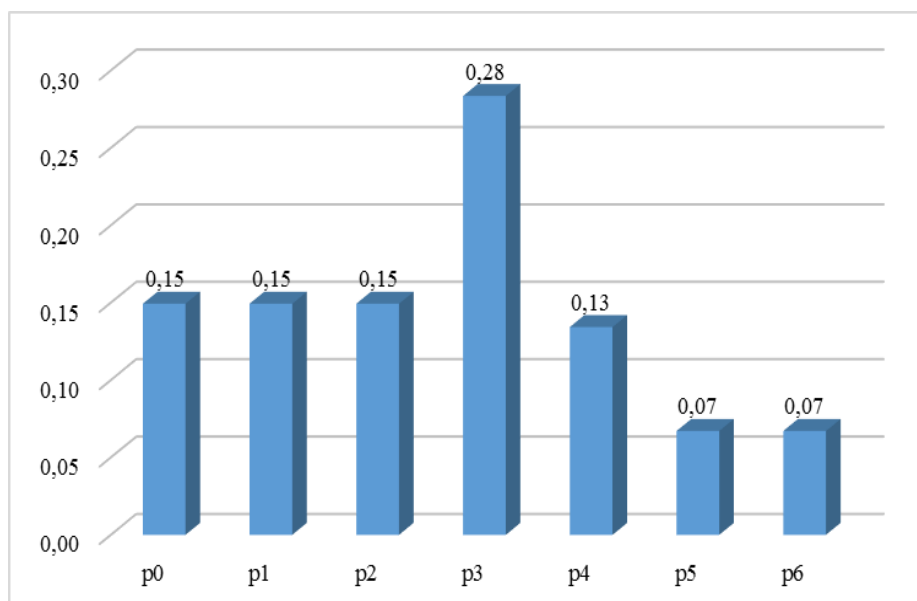


Рис. 7. Среднестатистические оценки финальных вероятностей на основе полного факторного плана стоимостей $a = 0,1 \div 1,0$ ($\Delta=0,1$) и $b = 0,3 \div 0,7$ ($\Delta=0,1$)

Графическая интерпретация, показанная на рисунке 8, связана с конкретной выборкой экспериментальных данных, селектированной для усредненной стоимости параметра b , связанного с направлением текущего запроса пользователя на авторизацию доступа к внешнему или внутреннему ресурсу (переходы t_6 и t_7 в PN-модели и соответственно переходы из состояния S_4 к S_5 и S_6 марковской цепи). Исследован случай равномерного распределения запросов между двумя ресурсами, при этом для параметра a , связанного с определением уровня легитимности запросов и/или приостановлением работы с системой, принято, что он меняется в диапазоне от 0,2 до 0,9 с шагом $\Delta=0,1$.

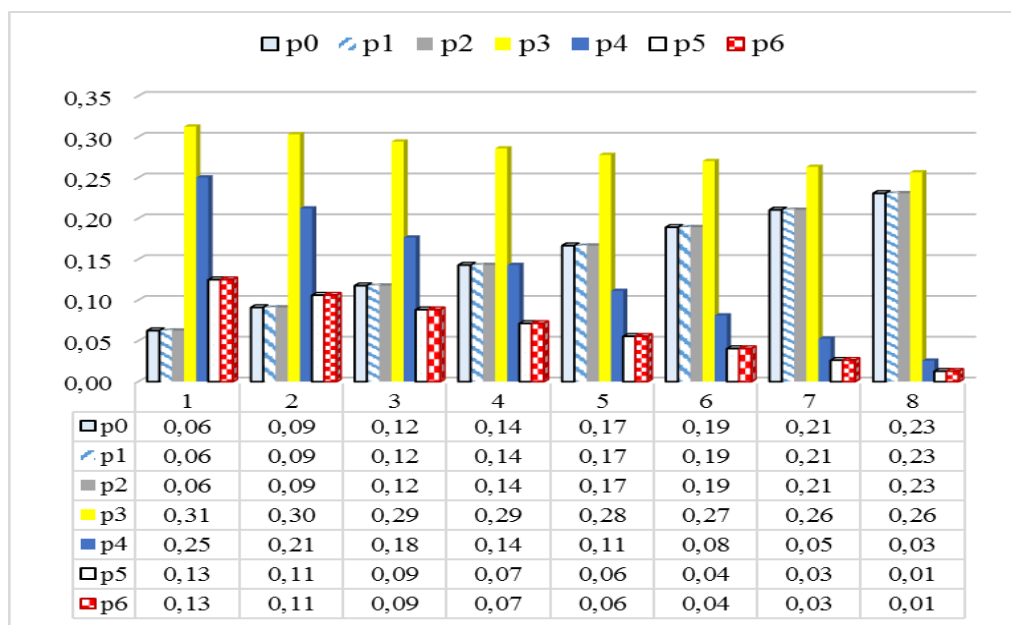


Рис. 8. Статистическая выборка финальных вероятностей при управляемых параметрах $b=0,5$ и $a=\{1=0,2; 2=0,3; 3=0,4; 4=0,5; 5=0,6; 6=0,7; 7=0,8; 8=0,9\}$

Оценки показывают, что самой высокой является стоимость вероятностей p_3 , соответствующая состоянию S_3 . Это состояние связано с переходами t_4 и t_5 , которые поддерживают процедуры по аутентификации и авторизации системы информационной безопасности. Оправдано равенство оценок вероятностей p_5 и p_6 по причине усредненной стоимости параметра b . Просматривается прямая зависимость тенденции уменьшения относительной занятости процедуры авторизации (вероятность p_4) с ростом стоимостей параметра a .

Заключение

В настоящей статье представлено расширение проведенного в [13] исследования функциональностей и процедур защиты информационных ресурсов в гетерогенной системе электронного образования с применением облачных технологий. В цитированной выше статье обсуждены особенности предлагаемой архитектуры комбинированной среды э-образования с использованием современных технологий цифрового мира, при этом сформулированы основные проблемы информационной безопасности и защиты персональной информации. В этом смысле во второй секции настоящей статьи представлено обобщение идеи, рассмотрены основные компоненты архитектуры и предлагается формализация процессов защиты информационных ресурсов, ориентированных на основную задачу – проведение модельного исследования процедур поддержки информационной безопасности в предлагаемой архитектуре.

Следующие две секции представляют собой разработанные модели – детерминированную и стохастическую, при этом предлагается их аналитическое решение. В случае со стохастической моделью выдвигается подход расширения детерминированного исследования (рис. 6) посредством сети Петри (рис. 4), а также представлена эволюция сети (рис. 5) с помощью марковской цепи. Это позволяет определить аналитические выражения вероятностей состояний при достижении

стационарного режима работы и с их помощью вычислить конкретные числовые стоимости при варьирующихся управляемых параметрах. В результате представлены полученные статистические оценки.

Одной из возможностей будущей работы по данной проблеме является проведение дополнительного статистического исследования, например, при помощи статистического софтвера DEVELVE (<http://develve.net/>).

Литература

1. Курейчик, В. В., А.А. Лежебоков, С.В. Пашенко. Новый подход к виртуальному обучению. Открытое образование. — 2014. — № 3. — с. 4-9.
2. Neville, K., C. Heavin. Using Social Media to Support the Learning Needs of Future IS Security Professionals. *Electronic Journal of e-Learning*. — 2013. — № 1 (vol. 11). — P. 29-38.
3. Joshi, N. A. Performance-Centric Cloud-Based e-Learning. *The IUP Journal of Information Technology*. — 2014. — № 2. — P. 7-16.
4. Альбекова З.М. Системы электронного образования и облачные технологии в образовании // Историческая и социально-образовательная мысль. — 2016. — № 1. — С. 5-7. URL: <http://cyberleninka.ru/article/n/sistemy-elektronnogo-obrazovaniya-i-oblachnye-tehnologii-v-obrazovanii#ixzz4dpJmSR52D>.
5. Рогальский Е. С. Облачные технологии и их роль в развитии электронного обучения. Исследования наукограда. — 2014. — № 1 (7). — С. 42-49. URL: <http://cyberleninka.ru/article/n/oblachnye-tehnologii-i-ih-rol-v-razvitii-elektronnogo-obucheniya>.
6. Nehru, V., M. Anto Bennet. An Architectural-Model for the Mobile based E-Learning Environment. *International Journal of Computer Science and Mobile Applications*. — 2014. — № 2 (vol.11). — P. 41-48. URL: http://www.academia.edu/9186926/An_Architectural-Model_for_the_Mobile_based_E-Learning_Environment.
7. Masud, M. A. H., X. Huang. An E-learning System Architecture based on Cloud Computing. *World Academy of Science, Engineering and Technology*. — 2012. — № 62. — P. 74-78.
8. Liao, J. et all. Collaborative Cloud: a New Model for e-Learning. *Innovations in Education and Teaching International*. — 2014. — № 3 (vol.51). — P. 338-351. URL: <http://www.tandfonline.com/doi/abs/10.1080/14703297.2013.791554>.
9. Евдокимов А. А., Э. Е. Тихонов. Защита данных в облачных технологиях. Монография. — Издательство НИЭУП, 2015. — 102 с. URL: <https://books.google.bg/books?id=kyXSCwAAQBAJ&>
10. Fischer, A. E. Improving User Protection and Security in Cyberspace // *Report of Committee on Culture, Science, Education and Media*, Council of Europe, 12.03.2014. URL: www.statewatch.org/news/2014/mar/coe-parl-ass-cyberspace-security.pdf.
11. Gamalel-Din, S., R. Salama, M. Al-Sowaiel. An Expert Consultant for Cloudifying E-Learning Environments // 2nd Int'l Conference on Future Internet of Things and Cloud (Barcelona, 27 August 2014). Spain, 2014. — P. 308-315.
12. Liang Hong, Changyuan Gao. Partner Selection of Cloud Computing Federation Based on Markov Chains. *Computer Modelling & New Technologies*. — 2014. — № 12B (vol.18). — P. 590-594. URL: (<http://www.cmnt.lv/en/on-line-journal/2014/2014-volume-18-12/part-b-information-and-computer-technologies/partner-selection>).
13. Romansky, R., I. Noninska. Architecture of Combined e-Learning Environment and Investigation of Secure Access and Privacy Protection. *International Journal of Human*

- Capital and Information Technology Professionals. — 2016. — № 3. — P. 89-106.
DOI: 10.4018/IJHCITP.2016070107
<http://www.igi-global.com/journal/international-journal-human-capital-information/1152>.
14. Romansky, R., I. Noninska. Globalization and Digital Privacy. Electrotechnika & Electronica (E+E), Bulgaria. — 2015. — No 11/12 (vol.50). — P. 36-41. URL: <http://ceec.fnts.bg/journal.html>).
 15. Аксёнов, В. G-Cloud: Архитектура, защита информации и выполнение требований законодательства при переносе информационных систем в „облако“ // Technology, 27.09.2016. — 15 с. URL: <https://www.slideshare.net/ActiveCloud/gcloud-66464615> (дата обращения 10.04.2017).
 16. Иванченко, О. В., В. С. Харченко. Анализ стохастических методов метамоделирования и оценивания готовности облачных инфраструктур. Радіоелектронні і компютерні системи. — 2016. — № 6 (80). — С. 6-11.
 17. Romansky, R., I. Noninska. An Approach for Modelling of Security Procedures for Information Resources Protection // International Advanced Research Journal in Science, Engineering and Technology. — 2016. — № 6. — P. 1-6. DOI 10.17148/IARJSET.2016.3601. URL: <http://www.iarjset.com/volume-3-issue-6>.