ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ, ИНФОРМАЦИОННО-СПРАВОЧНЫЕ, ЭКСПЕРТНО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ

УДК 004.75, 519.876.5

ИССЛЕДОВАНИЕ СЕРВИСА АНОНИМНОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ ШКОЛЫ

Статья поступила редакцию 28.09.2014, в окончательном варианте 11.12.2014.

Кравец Алла Григорьевна, профессор, доктор технических наук, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. им. В.И. Ленина, 28, e-mail: agk@gde.ru

Ле Суан Куен, аспирант, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. им. В.И. Ленина, 28, e-mail: lexuanquyen@gmail.com

В ходе проведенного исследования были выявлены недостатки в применении инструментов социальной оценки, связанные с низким уровнем конфиденциальности в социальных сетях. Поэтому в данной статье предложена процедура анонимной идентификации пользователей социальной сети с помощью специфической услуги псевдонима. Процедура анонимной идентификации проиллюстрирована на примере использования псевдонима пользователей для оценки качества лекций в социальной сети средней школы. Показаны преимущества и недостатки алгоритмов аутентификации на базе расширенной концепции Proof-Carrying Authorization, билинейного отображения и алгоритма Groth-Sahai. Проведено моделирование сервиса оценки качества лекции в виде сети массового обслуживания и разработан соответствующий алгоритм имитационного моделирования. Вычислительный эксперимент показал, что предложенный алгоритм использования псевдонима пользователей социальной сети школы не требует увеличения вычислительных мощностей. Этот алгоритм может быть применен для реализации любых процедур, требующих социальной оценки различных объектов.

Ключевые слова: социальная сеть, информационная безопасность, доказательство с нулевым разглашением, конфиденциальность, анонимность, аутентификация, система массового обслуживания, имитационное моделирование

RESEARCH OF ANONYMOUS IDENTIFICATION SERVICE IN SCHOOL SOCIAL NETWORKS

Kravets Alla G., D.Sc. (Engineering), Professor, Volgograd State Technical University, 28 Lenin Avenue, Volgograd, 400005, Russian Federation, e-mail: agk@gde.ru

Le Suan Kuen, post-graduate student, Volgograd State Technical University, 28 Lenin Avenue, Volgograd, 400005, Russian Federation, e-mail: lexuanquyen@gmail.com

In this article we present a procedure of social network users anonymous identification via specific service pseudonym. The research identified weaknesses in the application of the tools of the social assessment related to an insufficient level of privacy in social networks. The procedure is illustrated by the example of anonymous users' identifier service to evaluate lectures in a school social network. We developed authentication algorithms based on the extended concept Proof-Carrying Authorization, bilinear mapping and Groth-Sahai algorithm. Evaluated modeling services in the form of queuing networks and algorithm simulation services lectures was developed. Numerical experiments show that the proposed algorithm using users' pseudonym of the school social network does not require increasing computational power and can be implemented to any procedures requiring social assessment.

Keywords: social network, zero-knowledge proof, privacy, anonymity, authentication, queuing system simulation

Введение. На протяжении последних лет онлайновые социальные сети (on-line social networks – OSN) стали естественными средствами для обеспечения взаимодействия с людьми; участия в ряде общественных мероприятий, таких как обмен информацией, обмен мнениями и др. [12]. Сегодня большинство школьников общаются в социальных сетях, а многие школы организуют OSN сервисы внутри школьного сообщества. Услуги, которые предоставляются в таких сервисах, достаточно разнообразны: он-лайн чаты, дискуссионные комнаты, консультации, лекции, а также обмен документами, тестирование и другие аналогичные функции [1, 2, 7, 15]. Внутри таких социальных сетей осуществляют информационное взаимодействие школьники и их родители (опекуны), учителя, школьный персонал (библиотечный, медицинский и др.) [6]. Главная проблема, которая существует в таких социальных сетях, – это повышение конфиденциальности он-лайн общения и обсуждения личных проблем между пользователями [17]. Когда ученик сталкивается с проблемой, будь то физическая, психологическая, интеллектуальная, финансовая или любая другая, он может воспользоваться анонимным идентификатором, чтобы обсудить ее в социальной сети школы со своим учителем, консультантом или школьной медсестрой. В условиях, когда ученики могут быть уверены, что их анонимность хорошо защищена, консультант может убедиться, что пользователь действительно является учеником школы и имеет право на доступ к соответствующему сервису. Оставаясь анонимными, ученики могут быть более склонны говорить о реальных проблемах, с которыми они сталкиваются или могут столкнуться. В противном случае ученик может обсуждать проблему неохотно – в силу застенчивости, стыда или страха. Мы проиллюстрируем использование анонимного идентификатора пользователей (псевдонима) на примере задачи оценки качества (доступности, полезности и других характеристик) лекции в социальной сети школы.

Теоретический базис работы

Инструменты оценки в социальных сетях. На сегодняшний день одним из наиболее эффективных средств повышения качества обучения является обеспечение обратной связи с учениками. Для выяснения мнений учащихся применяются как уже давно устоявшиеся методы (анкетирование, опрос и др.), так и новые, еще недостаточно изученные способы (социальная оценка, анонимное голосование, оценка отдельных видов учебной деятельности). Размещение обучающих материалов в сети Интернет, использование систем дистанционного обучения [3] и – главное – возможность включения в такие системы инструментов социальной оценки позволяют получить отклик от учеников наиболее оперативно и в виде, пригодном для дальнейшей аналитической обработки [4, 5, 16], в том числе в автоматизированной форме. К таким инструментам оценки можно отнести следующие:

- «лайк» – самая простая социальная оценка, означающая поддержку (одобрение) размещенного в социальной сети материала;
- «коммент» – сообщение, содержащее текстовую и/или аудиовизуальную информацию, в котором автор «коммента» выражает свое мнение по поводу размещенного в социальной сети материала;
- «репост» – перенос материала или ссылки на материал на свою личную страницу (профиль) социальной сети.

При этом необходимо отметить следующие недостатки в применении инструментов социальной оценки в OSN.

1. Автор материала может предоставить доступ к нему, возможность оценивать и комментировать его пользователям определенных категорий (например, «друзьям») или пользователям, входящим в определенное сообщество («группу»). При этом профили пользователей должны быть «открыты» для автора материала.

2. Пользователь должен войти в свой профиль социальной сети для того, чтобы иметь возможность оценивать материалы, размещенные другими пользователями. В некото-

рых OSN предусмотрена возможность просмотра некоторых материалов под «гостевым» доступом (без авторизации в сети), но оценивать материал «гость» не может.

Таким образом, существующие механизмы социальной оценки [13] могут быть применимы в социальной сети школы с целью оценки учебных материалов (лекций) учениками. Однако для этого необходимо разработать алгоритмы и средства анонимной идентификации пользователя. Применение псевдонимов позволит получить более объективную оценку качества лекций со стороны учеников.

Авторизация ученика. Proof-Carrying Authorization (PCA) успешно применяется в контексте WEB-приложений, мобильных устройств. Maffei и Pecina [18] расширили концепцию PCA на основе комбинации цифровой подписи и алгоритма доказательства с нулевым разглашением (ДНР). В цифровой подписи использовано обоснование, базирующееся на логических формулах, в алгоритме ДНР – выбор конфиденциальности данных. Расширение PCA поддерживает различные свойства конфиденциальности – такие как секретность данных и анонимность пользователей. Расширение PCA построено на стандарте логики высшего порядка.

На рис. 1 представлена схема взаимодействия между учениками и сервисным центром для получения *Id*.

SIGNED

$$\frac{\Gamma \mapsto digital\_signature(s, A, F)}{\Gamma \mapsto A \ says \ F}$$

NAME - IMP - E

$$\frac{A \ says \ F \quad A \ says \ F \rightarrow G}{A \ says \ G}$$

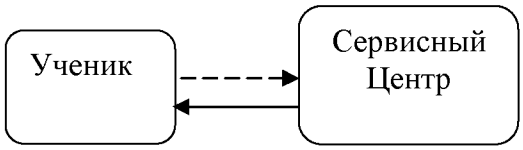

Рис. 1. Метод «says» – регистрация услуги

Сервер использует данное взаимодействие для получения личной информации об учащемся, такой как имя, класс, серийный номер ученика, возраст, пол, адрес, дата рождения, географическое положение (место проживания), номер телефона и др.

По полученному *id* будет сгенерирован личный и публичный ключ для дальнейшего взаимодействия. Личный ключ ученика будет использован, чтобы построить утверждение: *ID says RegisterReq(Prof)*. На рис. 2 представлена процедура получения ответа от сервисного центра ученику в виде: $sign(Registered(ID,Course))_{skprof}$ или утверждения:
Prof says Registered(ID, Course).

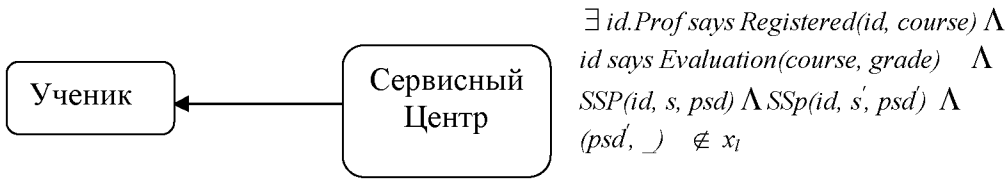

Рис. 2. Регистрация ученика для оценки лекций

На основе полученного ответа ученик сможет построить ответный запрос в виде утверждения:
$\exists$ *id.Prof says Registered(id, course)* Λ *id says Evaluation(course, grade)*

Специфическая услуга псевдонима. Специфическая услуга псевдонима (SSPs) разработана Matteo Maffei [19], чтобы гарантировать следующие свойства: уникальность, анонимность и независимость сервисов:

$SSP(id, s, psd) \Lambda SSP(id, s', psd') \Lambda (psd', \_) \notin x_1$.

Ученик будет доказывать утверждение на рис. 2 для сервисного центра. Если аутентификация утверждения была правильной, то сервисный центр возвратит результат возможности оценки лекций для ученика.

Криптографическая реализация. Криптографические примитивы, необходимые для сборки вышеупомянутого алгоритма ДНР, описаны в [14, 15, 16]. Использование билинейных отображений делает эти примитивы эффективными.

Билинейное отображение**.** В случае билинейного отображения [16] элементов $G_1 \times G_2$ в целевой группе G_T имеет место равенство для всех значений G,

$$H, x, y.\ e(x.G,y.H)=e(G,y.H)^x = e(x.G,H)^y = e(G,H)^{xy};\ G, H, x, y$$

где G – генератор; H – генератор; $x, y \in Z_n$; n – простое число.

Схема цифровой подписи. Мы используем схему цифровой подписи, которая была недавно предложена Abe [13]. Алгоритм Groth-Sahai ДНР SXDH (symmetric external Diffie-Hellman assumption) является очень гибким и имеет общую концепцию. Будем использовать систему доказательств Groth-Sahai [14–16] для разработки и реализации конфиденциальности материалов социальной сети.

Моделирование оценки лекций. Когда лекция загружена в социальную сеть школы, размещенную в Интернет, число возможных пользователей достаточно велико. Поэтому необходимо оценить производительность системы аутентификации.

Мы используем подход из [8] для моделирования процедуры оценки качества лекции (рис. 3).

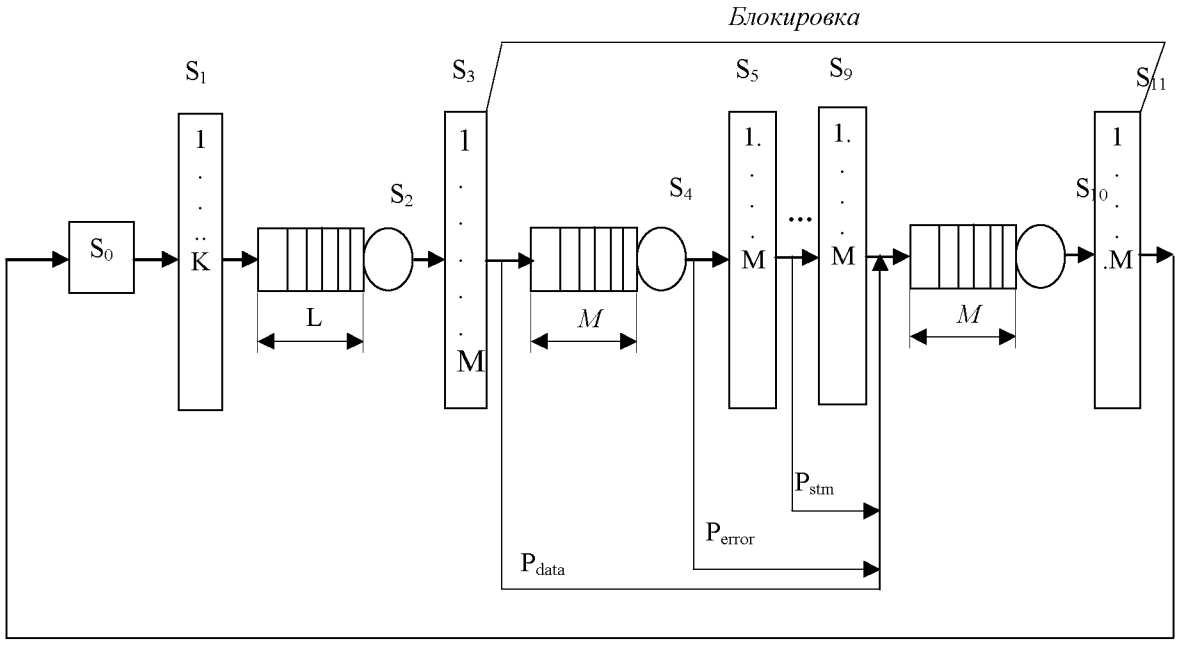

Рис. 3. Схема моделирования оценки лекции в виде сети массового обслуживания.

Обозначения на рис. 3 S_0 – длительность обслуживания в центре, S_0 распределена по экспоненциальному закону с параметром λ; S_1 – центр, формализующий работу модуля

TCP операционной системы на этапе установления соединения; «*M*» – число обслуживающих каналов, очередь отсутствует. Данный центр формализует работу модуля TCP операционной системы. В нем обрабатываются заявки клиентов на этапе установления соединения при осуществлении так называемого «трехэтапного рукопожатия». S_2 – основной поток приложения (оценка лекций) сервера, извлекающего заявки из очереди на установление соединения и осуществляющего создание дочерних потоков. Максимальная длина очереди L к центру задается в серверном приложении. S_3, S_{11} – эти центры имеют по «*M*» каналов обслуживания (потоков сервера) и при начале обслуживания заявки в i - M канале в центре S_3 он считается занятым до завершения обслуживания в i - M канале S_{11}. Таким образом, происходит блокировка каналов центров S_3, S_{11}. S_4 – центры, которые извлекают доказательства в блоках на рис. 2 для различных доказательств. S_4 – центр с длинной очереди M. S_5 – центр, формализующий работу аутентификации утверждения: *Prof says Registered(id, course).* S_6 – центр, формализующий работу по аутентификации утверждения: *id says Evaluation(course, grade)*. S_7 – центр, формализующий процесс аутентификации утверждения: *SSP(id, s, psd)*. S_8 – центр, формализующий работу аутентификации утверждения: *SSP(id, s′, psd′)*. S_9 – центр, формализующий работу проверки утверждения: *(psd′, _)* $\notin x_l$. S_{10} – центр, формализующий работу модуля генерации ответа сервера с длинной очереди M.

Дисциплины обслуживания центров приведены в табл. 1.

Таблица 1

Дисциплины обслуживания центров

Центр	Дисциплина обслуживания
S_1, S_3,S_5,S_6, S_{11}, S_7, S_8, S_9	IS (с обслуживанием без ожидания).
S_2	FCFS- M/M/1 (First come first served)
S_4,S_{10}	PS (разделение ресурсов процессора)

Алгоритм имитационного моделирования системы аутентификации в социальных сетях представлен на рис. 4. Алгоритм реализует предложенную схему моделирования оценки лекции в виде сети массового обслуживания.

Результаты имитационного моделирования оценки лекции. Моделирование оценки качества лекции производилось при помощи программы, разработанной на языке C# на основе приведенных выше алгоритмов для имитационной модели. Интерфейс программы моделирования представлен на рис. 5.

Пояснения к входным данным программы по рис.5. Интенсивность пуассоновского потока заявок λ = 0,1; 1.0 c^{-1} для каждого пользователя. Допустимое время установления TCP соединения – 20 с. Допустимое время ожидания обслуживания после установления TCP соединения – 20 с. Время извлечения заявки из очереди на обслуживание и создание дочернего потока серверным приложением – 0.12 с. Размер очереди заявок равен 80. Максимально количество потоков сервера M = 150. Длительности обработки для: RTT = 0.05, S_4=0.1, S_5=1.2, S_6 = 0.4, S_7 =0.4, S_8 = 0.3, S_9 = 0.2 с.

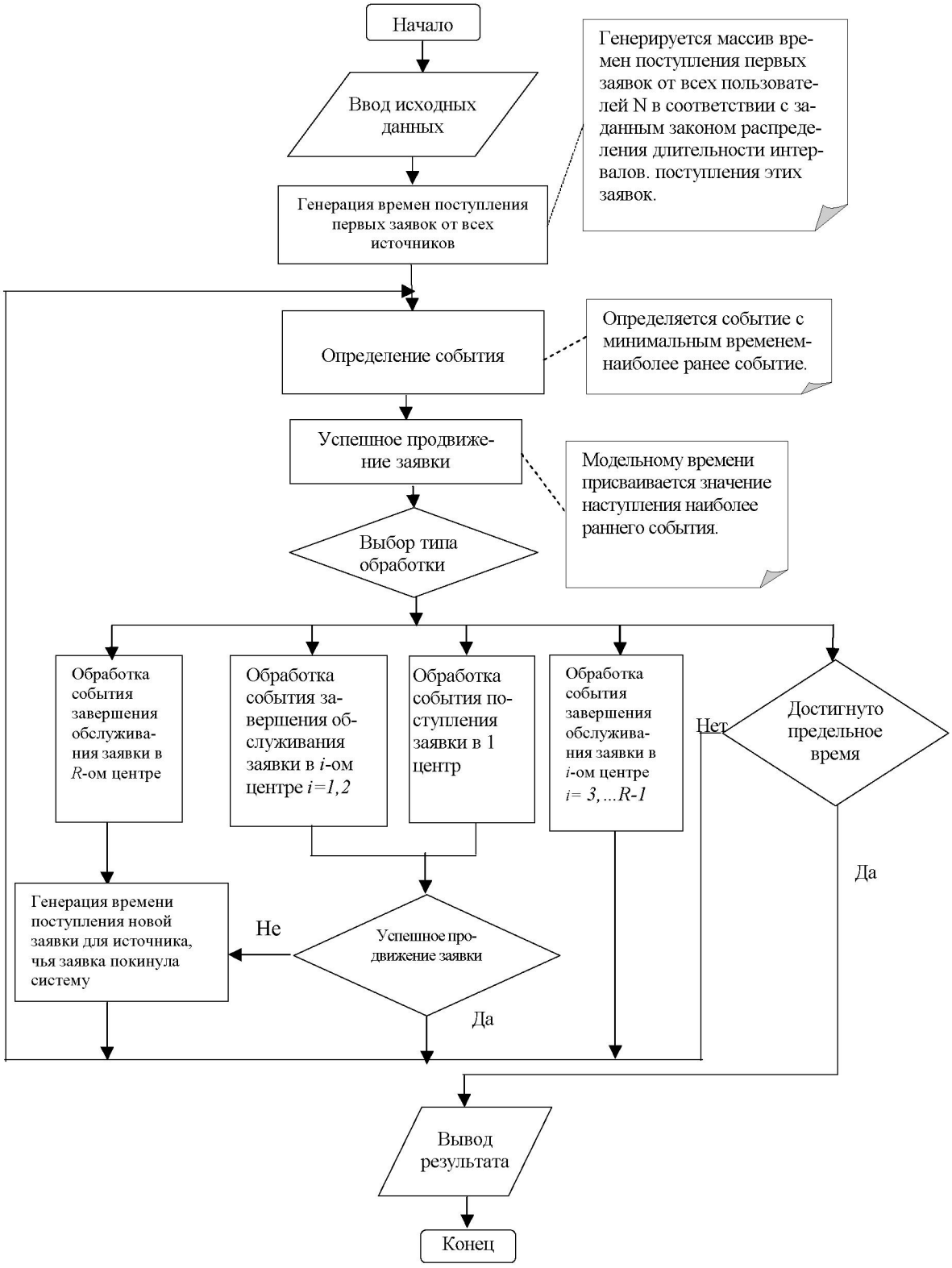

Рис. 4. Алгоритм имитационного моделирования системы аутентификации в социальных сетях

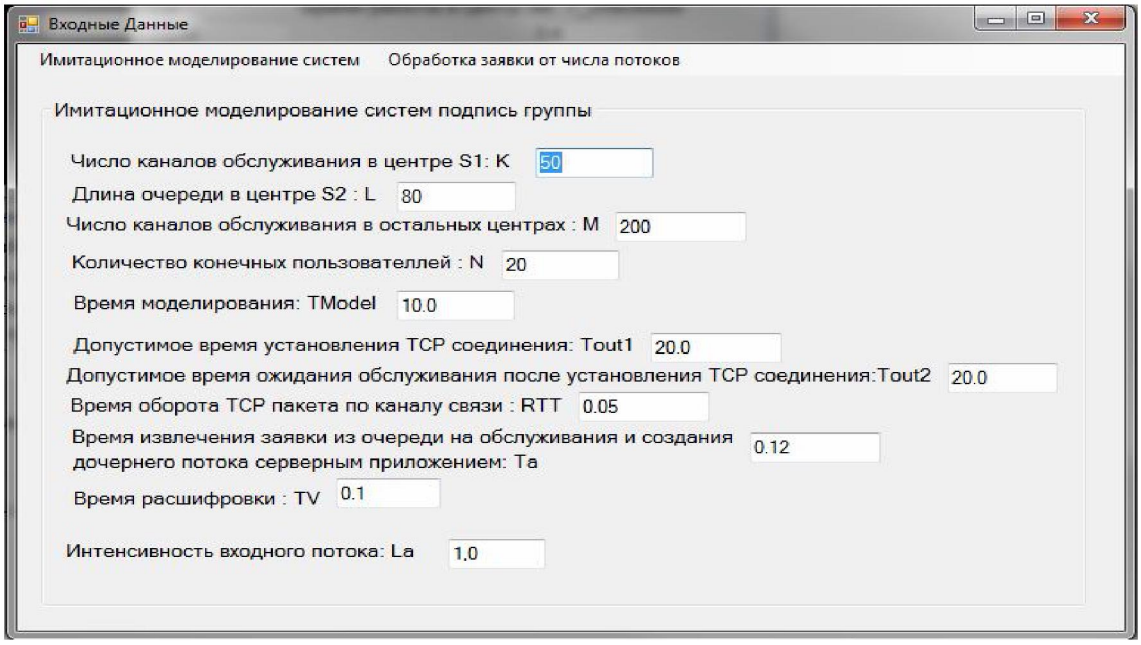

Рис. 5. Задание параметров моделирования в программе

На рис. 6 представлены результаты моделирования при максимальном количестве одновременно открытых сетевых соединений, равном 50.

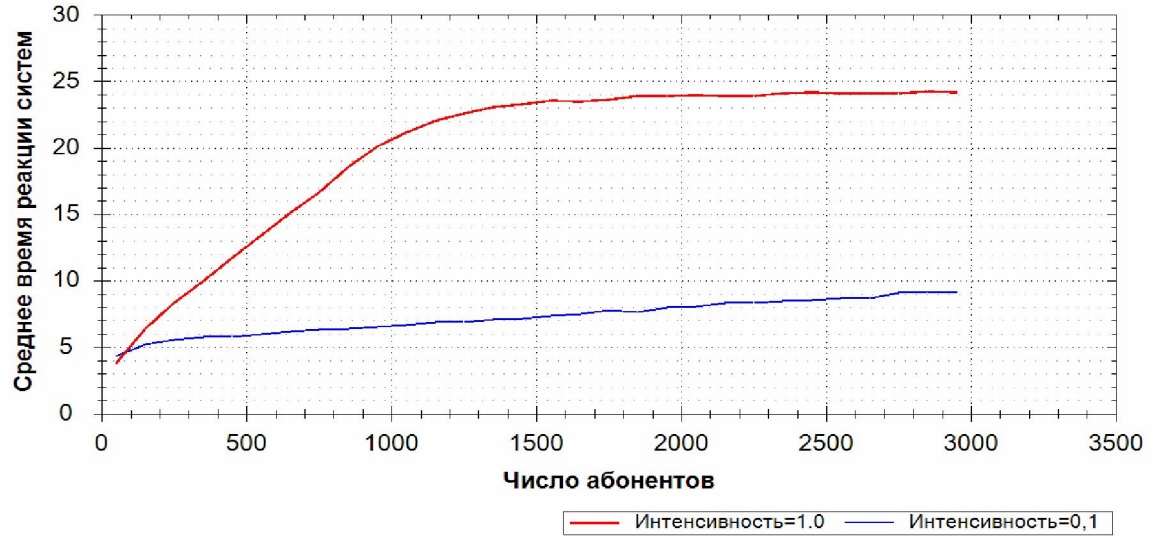

Рис. 6. Зависимость среднего времени обслуживания заявки
от количества абонентов системы

Зависимости коэффициентов потерь (количество потерь заявок / количество поступлений заявок) от количества абонентов в сети иллюстрирует рис. 7. Данные зависимости показывают, что вначале основной составляющей суммарных потерь являются потери из-за превышения допустимого времени ожидания начала обслуживания в центре S_3.

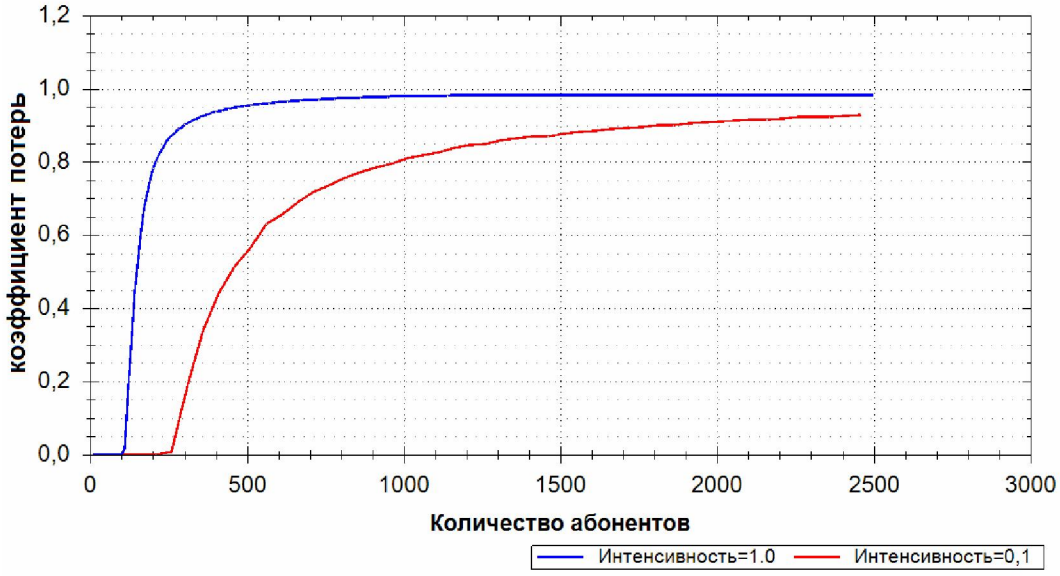

Рис. 7. Зависимость коэффициентов потерь от числа абонентов

Проведенный численный эксперимент показал, что при интенсивности пуассоновского потока $\lambda = 0.1$ c^{-1} не происходит накопления заявок в очереди сервера - поскольку количество потоков, выделяемых сервером для обслуживания заявок, не достигает максимального значения (1– 1999 абонентов). С дальнейшим ростом числа пользователей (от 2000 абонентов и более) возрастает интенсивность входящего потока; увеличивается и среднее время реакции системы – до 42 с и более.

Выводы. В социальных сетях процесс аутентификации пользователей является очень важным и сложным. На основе протокола специфической услуги псевдонима авторами был разработан модуль оценки лекции, в котором ученик имеет возможность анонимно осуществлять свои действия. Результат исследования был использован для построения плагинов (add-ons) в браузерах Firefox, Google Chrome и др. Таким образом, предложенный алгоритм использования псевдонима пользователей социальной сети школы не требует увеличения вычислительных мощностей локальной сети и потенциально может быть использован для реализации любых процедур социальной оценки различных объектов.

Список литературы

1. Адеянов И. Е. Современное состояние и пути развития системы образования : моногр. / И. Е. Адеянов, Р. А. А. Аль-Шаеби, А. М. Аронов и др. – Одесса, 2012. – Т. 1. – 176 с.

2. Гуртяков А. С. Организация дистанционного обучения / А. С. Гуртяков, А. Г. Кравец // Известия ВолгГТУ. Серия «Актуальные проблемы управления, вычислительной техники и информатики в технических системах». – 2012. – Вып. 13. – № 4 (91). – С. 103–107.

3. Гуртяков А. С. Система дистанционного проведения лекций / А. С. Гуртяков, А. Г. Кравец // Инновации на основе информационных и коммуникационных технологий (ИНФО-2012) : мат-лы 9-й Междунар. науч.-практ. конф., посвящ. 50-летию МИЭМ и 20-летию НИУ ВШЭ, Россия, г. Сочи, 1–12 окт. 2012 г. / МИЭМ НИУ ВШЭ [и др.]. – М., 2012. – С. 83–84.

4. Гуртяков А. С. Web 2.0 приложения в корпоративных системах дистанционного образования / А. С. Гуртяков, А. Г. Кравец // Сборник научных трудов SWorld. Научные исследования и их практическое применение. Современное состояние и пути развития `2012 : мат-лы Междунар. науч.-практ. конф., 2–12 окт. 2012 г. / Одес. нац. морской ун-т [и др.]. – Одесса, 2012. – Вып. 3, т. 5. Технические науки. – С. 55–59.

5. Гуртяков А. С. Фрактальная компетентностная архитектура корпоративных систем дистанционного образования / А. С. Гуртяков, А. Г. Кравец, Д. В. Юдин, А. Д. Кравец // Современные проблемы науки и образования : электрон. науч. журнал. – 2012. – № 3. – Режим доступа: http://www.science-education.ru/103-6238 (дата обращения 27.09.2014), свободный. – Загл. с экрана. – Яз. рус.

6. Исаев А. В. Автоматизированная система поддержки учебной траектории: определение функциональных ролей и их соподчинение / А. В. Исаев, А. Г. Кравец, М. П. Мельников // Изв. ВолгГТУ. Серия «Актуальные проблемы управления, вычислительной техники и информатики в технических системах». – 2011. – Вып. 12, № 11. – С. 84–88.

7. Исаев А. В. Современные тенденции построения общеобразовательных программ / А. В. Исаев, А. Г. Кравец // Современные проблемы и пути их решения в науке, транспорте, производстве и образовании` 2009 : сб. науч. тр. по мат-лам Междунар. науч.-практ. конф., 21–28 декабря 2009 г. / Одес. нац. морской ун-т [и др.]. – Одесса, 2009. – Т. 16. – С. 65–72.

8. Лукьянов В. С. Модели компьютерных сетей с удостоверяющими центрами : моногр. / В. С. Лукьянов, И. В. Черковский, А. В. Скакунов, Д. В. Быков. – Волгоград, 2009. – 241 с.

9. Abe M. Structure-preserving signatures and commitments to group elements / M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev and M. Ohkubo // Springer – CRYPTO. – 2010. – Vol. 6223 of LNCS. – P. 209–236.

10. Blazy A. Batch Groth-Sahai / A. Blazy, G. Fuchsbauer, M. Izabach` ene, A. Jambert, H. Sibert, and D. Vergnaud // ACNS'10 : Proceedings of the 8th International Conference on Applied Cryptography and Network Security. – 2010. – P. 218–235.

11. Chumak A. A. Analysis of User Profiles in Social Networks / A. A. Chumak, S. S. Ukustov, A. G. Kravets // Knowledge-Based Software Engineering : Proceedings of 11th Joint Conference, JCKBSE 2014 (Volgograd, Russia, September 17–20, 2014) / ed. by A. Kravets, M. Shcherbakov, M. Kultsova, Tadashi Iijima ; Volgograd State Technical University [etc.]. – Springer International Publishing, 2014. – P. 70–76. – (Series: Communications in Computer and Information Science ; Vol. 466).

12. Chumak A. A. Social Networks Message Posting Support Module / A. A. Chumak, S. S. Ukustov, A. G. Kravets, Yu. F. Voronin // World Applied Sciences Journal (WASJ). – 2013. – Vol. 24, spec. issue 24: Information Technologies in Modern Industry, Education & Society. – P. 191–195.

13. Ghadafi E. Groth-Sahai proofs revisited / E. Ghadafi, N. P. Smart and B. Warinschi // Springer-Public Key Cryptography – PKCS 2010. – 2010. – P.177–192.

14. Groth J. Efficient Non-interactive Proof Systems for Bilinear Groups / J. Groth and A. Sahai // Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). – 2010. – № 8.– P. 415–430.

15. Isaev A. V. Distance education: educational trajectory control / A. Isaev, L. Isaeva, A. Kravets, S. Fomenkov // Multi Conference on Computer Science and Information Systems 2013 (Prague, Czech Republic, July 23–26, 2013) : Proceedings of the International Conference e-Learning 2013 / IADIS (International Association for Development of the Information Society). – Prague, 2013. – P. 151–158.

16. Isaev A. V. Individualized Educational Trajectory: Educational Courses Integration / A. Isaev, L. Isaeva, A. Kravets // World Applied Sciences Journal (WASJ). – 2013. – Vol. 24, spec. issue 24: Information Technologies in Modern Industry, Education & Society. – P. 62–67.

17. Le Xuan Quyen. Development of a Protocol to Ensure the Safety of User Data in Social Networks, Based on the Backes Method / Le Xuan Quyen, Alla G. Kravets // Knowledge-Based Software Engineering : Proceedings of 11th Joint Conference, JCKBSE 2014 (Volgograd, Russia, September 17–20, 2014) / ed. by A. Kravets, M. Shcherbakov, M. Kultsova, Tadashi Iijima ; Volgograd State Technical University [etc.]. – Springer International Publishing, 2014. – P. 393–399. – (Series: Communications in Computer and Information Science ; Vol. 466).

18. Maffei M. Privacy-Aware Proof-Carrying Authorization / M. Maffei and K. Pecina // ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS'11). – 2011. – № 7. – P. 87–95.

19. Maffei M. Security and Privacy by Declarative Design / Maffei M., Saarland Univ., Saarbrucken // IEEE – Computer Security Foundations Symposium (CSF). – 2013. – № 26. – P. 81–96.

References

1. Adeyanov I. Ye, Al-Shaebi R. A. A., Aronov A. M. et al. *Sovremennoe sostoyanie i puti razvitiya sistemy obrazovaniya* [Educational system modern state and development ways]. Odessa, 2012, vol. 1, p. 176.

2. Gurtyakov A. S., Kravets A. G. Organizatsiya distantsionnogo obucheniya [Distant learning organization]. *Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta* [News of Volgograd State Technical University], 2012, vol. 4, no. 13, pp. 103–107.

3. Gurtyakov A. S., Kravets A. G. Sistema distantsionnogo provedeniya lektsiy [System of distant lecturing]. *Innovatsii na osnove informatsionnykh i kommunikatsionnykh tekhnologiy* [Innovations on the basis of information and communication technologies], 2012, no. 1, pp. 83–84.

4. Gurtyakov A. S., Kravets A. G. Web 2.0 prilozheniya v korporativnykh sistemakh distantsionnogo obrazovaniya [WEB 2.0 applications in corporate systems of distance education]. *Sbornik nauchnykh trudov Sworld ' 2012* [Proceedings Sworld ' 2012], 2012, iss. 3, vol. 5, pp. 55–58.

5. Gurtyakov A. S., Kravets A. G., Yudin D. V., Kravets A. D. Fraktalnaya kompetentnostnaya arkhitektura korporativnykh sistem distantsionnogo obrazovaniya [Fractal competence architecture of corporate distance education systems]. *Sovremennye problemy nauki i obrazovaniya* [Modern Science and Education Problems], 2012. Available at: http://www.science-education.ru/103-6238 (accessed 27 September 2014).

6. Isaev A. V., Kravets A. G., Melnikov M. P. Avtomatizirovannaya sistema podderzhki uchebnoy traektorii: opredelenie funktsionalnykh roley i ikh sopodchinenie [Automated support system training path: the definition of the functional roles and their subordination]. *Izvestiya Volgogradskogo gosudarstvennogo tehnicheskogo universiteta* [News of Volgograd State Technical University], 2011, vol. 11, no. 12, pp. 84–88.

7. Isaev A. V., Kravets A. G. Sovremennye tendentsii postroeniya obshcheobrazovatelnykh programm [Modern trends in the education programs construction]. *Sovremennye problemy i puti ikh resheniya v nauke, transporte, proizvodstve i obrazovanii` 2009: sbornik nauchnykh trudov* [Modern problems and ways of their solution in science, transport, production and education ' 2009: Proceedings]. Odessa, 2009, vol. 16, pp. 65–71.

8. Lukyanov V. S., Cherkovskiy I. V., Skakunov A. V., Bykov D. V. *Modeli kompyuternykh setey s udostoveryayushchimi tsentrami* [Models of computer networks with certifying centers]. Volgograd, 2009. 241 p.

9. Abe M., Fuchsbauer G., Groth J., Haralambiev K., Ohkubo M. Structure-preserving signatures and commitments to group elements. *Springer – CRYPTO*, 2010, vol. 6223 of LNCS, pp. 209–236.

10. Blazy A., Fuchsbauer G., Izabach` ene M., Jambert A., Sibert H., Vergnaud D. Batch Groth-Sahai. *ACNS'10 Proceedings of the 8th international conference on Applied cryptography and network security*, 2010, pp. 218–235.

11. Chumak A. A., Ukustov S. S., Kravets A. G. Analysis of User Profiles in Social Networks. *Knowledge-Based Software Engineering : Proceedings of 11th Joint Conference, JCKBSE 2014* (Volgograd, Russia, September 17–20, 2014). Springer International Publishing, 2014, pp. 70–76. (Series: Communications in Computer and Information Science; vol. 466).

12. Chumak A. A., Ukustov S. S., Kravets A. G., Voronin Yu. F. Social Networks Message Posting Support Module. *World Applied Sciences Journal (WASJ)*, 2013, vol. 24, spec. issue 24: Information Technologies in Modern Industry, Education & Society, pp. 191–195.

13. Ghadafi E., Smart N. P., Warinschi B. Groth-Sahai proofs revisited. *Springer-Public Key Cryptography – PKCS 2010*, 2010, pp. 177–192.

14. Groth J., Sahai A. Efficient Non-interactive Proof Systems for Bilinear Groups. *Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, 2010, no. 8, pp. 415–430.

15. Isaev A., Kravets A., Isaeva L., Fomenkov S. Distance education: educational trajectory control. *Multi Conference on Computer Science and Information Systems 2013 (Prague, Czech Republic, July 23–26, 2013): Proceedings of the International Conference e-Learning 2013*. Prague, 2013, pp. 151–158.

16. Isaev A. V., Isaeva L. A., Kravets A. G. Individualized educational trajectory: educational courses integration. *World Applied Sciences Journal*, 2013, vol. 24, no. 24, pp. 62–67.

17. Le Xuan Quyen and Alla G. Kravets. Development of a Protocol to Ensure the Safety of User Data in Social Networks, Based on the Backes Method. *Knowledge-based software engineering. Communications in Computer and Information Science*, Springer, 2014, vol. 466, pp. 393–399.

18. Maffei M. and K. Pecina Privacy-Aware Proof-Carrying Authorization. *ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS'11)*, 2011, no. 7, pp. 87–95.

19. Maffei M., Saarland Univ., Saarbrucken. Security and Privacy by Declarative Design. *IEEE – Computer Security Foundations Symposium (CSF)*, 2013, no. 26, pp. 81–96.