Компьютерные инструменты в образовании, 2015
№ 4: 52–60
УДК: 614.8+002.6:004.89
http://ipo.spb.ru/journal

АНАЛИЗ ЗАЩИЩЁННОСТИ ГРУПП ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК: ПРИНЦИП И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ*

Азаров Артур Александрович, Абрамов Максим Викторович,
Тулупьева Татьяна Валентиновна, Тулупьев Александр Львович

Аннотация

Актуальной задачей анализа защищенности пользователей является разбиение пользователей информационной системы на группы, например, соответствующие удаленным офисам организации, и анализ таких групп пользователей. В статье представлен один из модулей прототипа программного комплекса, реализующий анализ защищенности пользователей информационных систем от социоинженерных атак.

Ключевые слова: *информационная безопасность, социоинженерные атаки, пользователи, информационная система, конфиденциальная информация.*

1. ВВЕДЕНИЕ

Задачи защиты информации в настоящее время являются одними из наиболее приоритетных [3]. Они решаются не только органами государственного, регионального и местного управления, но и коммерческими предприятиями в различных отраслях производства и сфере услуг. Защита информации в компьютерной сети обладает своей спецификой, обусловленной разнообразием угроз информационной безопасности. Актуальность данной тематики подчёркивается статистикой последних лет, которая демонстрирует увеличение количества атак на информационные системы, рост времени, необходимого для расследования таких преступлений, и размеров ущерба, нанесенного компаниям, атаки на которые увенчались успехом. Исследование 2014 года, охватившее семь стран, показало, что средний размер убытков американских компаний от киберпреступлений вырос более чем на 9%, до 12,7 миллиона долларов. В исследовании за 2013 год это значение составляло 11,6 миллиона долларов. Среднее время, необходимое для расследования атаки на информационные системы, также выросло, теперь оно составляет 45 дней по сравнению с 32 днями в 2013 году [20].

До сих пор большая часть исследований в области защиты информации посвящена усовершенствованию программно-технических компонент, обеспечивающих

*Статья содержит материалы, полученные в проектах, частично поддержанных грантами РФФИ №№ 10-01-00640-а, 14-07-00694-а, 15-01-09001-а, грантом СПбГУ № 6.38.72.2011.

безопасность конфиденциальных данных [1, 5, 12, 13]. В таком срезе вопросы информационной безопасности достаточно хорошо изучены, разработано большое количество средств, позволяющих свести к минимуму вероятность успеха программно-технической атаки злоумышленника. В то же время действия пользователей информационных систем играют существенную роль в системе защиты информации [16]. Пользователь информационной системы, к данным которой злоумышленник пытается получить доступ, является одним из ее самых уязвимых мест. В [11] отмечается, что наиболее распространённые инциденты информационной безопасности так или иначе связаны с действиями пользователей информационных систем. Одним из наиболее эффективных видов атак на информационную безопасность является корпоративный шпионаж, которому подвергаются более четверти компаний: почти 80% известных случаев проведения промышленного шпионажа закончились успешно для злоумышленника, а компании, по отношению к которым реализовывалось данное воздействие, получили убытки [11].

Сотрудник компании, имеющий доступ к конфиденциальной информации, может преднамеренно или непреднамеренно нарушить её безопасность (конфиденциальность, целостность или доступность) [17, 18]. В [10] отмечается, что санкционированный пользователь информационной системы вероятнее всего знаком с рядом сотрудников, обслуживающих и администрирующих информационную систему; имеет ряд разрешений на доступ к документам, хранящимся в информационной системе; может знать парольную информацию коллег; обладает физическим доступом к некоторым компьютерам. В связи с этим, взаимодействие пользователей информационной системы со злоумышленниками может нанести серьёзный ущерб компании.

Актуальность исследований в данной области подчёркивается также особенностью социоинженерных атак, которая заключается в том, что им в равной степени могут быть подвержены люди, обладающие разными уровнями компетенций и подготовки [4, 6, 7]. Данный тезис подтверждается некоторыми эпизодами социоинженерных атак, получившими известность в последнее время. Так в начале 2013 года американский технический специалист, бывший сотрудник ЦРУ и АНБ Эдвард Сноуден похитил 1,7 миллиона секретных файлов специальных служб США и значительную часть из них передал газетам The Guardian и The Washington Post [14]. Позже один инцидент нарушения конфиденциальности информации был зафиксирован на еще более высоком уровне. Он произошёл в октябре 2015 года. Подросток, используя методы социальной инженерии, получил доступ к почте директора ЦРУ США Джона Бреннана [15].

Успешная атака на информационную систему может приводить к существенным последствиям, выражающимся в разных формах. В России средний ущерб от серьёзного инцидента для компаний, относящихся к сегменту малого и среднего бизнеса, составляет 780 000 рублей, для крупных предприятий эта сумма может достигать 20 миллионов рублей [11].

Таким образом, проблемы информационной безопасности и защиты пользователей от социоинженерных атак в настоящее время становятся все актуальнее. Исследования в этой области помогут в создании многоуровневых систем безопасности, более устойчивых к атакам злоумышленников.

Целью данной статьи является описание базирующегося на анализе вероятности сложного события принципа построения оценки защищенности пользователя по отношению к атакующим действиям злоумышленника, причем в силу ограничений экспериментальной базы — результатов соответствующего пилотного исследования [17] — рассматриваются действия достаточно элементарного характера («одноходов-

ки»), нацеленные на «элементарные» уязвимости пользователя, воздействие на которые приводит непосредственно к какому-то действию пользователя. Кроме того, в качестве иллюстрирующего примера использования предложенного принципа приведен программный модуль, поддерживающий анализ защищенности групп пользователей информационных систем.

2. ПОСТРОЕНИЕ ПРОФИЛЯ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЯ

Для решения задачи анализа защищенности пользователей информационных систем перспективным представляется формирование профиля уязвимостей пользователя. Существует ряд баз данных, содержащих уязвимости программно-технических компонент информационных систем, но не существует аналогичных баз данных уязвимостей пользователей. Последние уязвимости, очевидно, не являются программно-техническими и носят совершенно иной характер [2]. В силу того что уязвимости пользователей не наблюдаются напрямую, представляется целесообразной разработка подходов к формированию косвенной оценки (или косвенных оценок) степени выраженности уязвимостей. В частности, была выдвинута гипотеза, что одну из таких косвенных оценок можно получить на основе результатов психологических тестов, предназначенных для оценки степени выраженности психологических особенностей личности. Для подтверждения гипотезы было проведено уже упоминавшееся исследование, носившее пилотный характер [19].

В ходе исследования было выявлено пять уязвимостей пользователя, степень выраженности которых оказалась взаимосвязана со степенью выраженности психологических особенностей личности:

- *Техническая неосмотрительность.* Пользователь имеет низкую самооценку по внешности, низкая потребность в новых ощущениях, низкий уровень средней самооценки.
- *Слабый пароль.* Пользователь склонен к безалаберности, невнимательности, в том числе и по отношению к безопасности своих идентификационных данных. У него высокий уровень подозрительности, он очень самоуверен. Вместе с тем у него плохая слуховая память и он ярко выраженный меланхолик.
- *Техническая халатность и установка на получение личной выгоды.* Пользователь подозрителен, у него высокая самооценка по авторитету у сверстников, он дипломатичен, не склонен переживать из-за каких-либо проблем. В то же время он ставит перед собой нереальные цели в умении делать многое своими руками и, наоборот, очень скромно оценивает свои возможности в уверенности в себе, у него низкая склонность к риску, он не мстителен и недооценивает свои умственные возможности.
- *Техническая неопытность.* Пользователь обладает высоким вытеснением и рационализацией, то есть он невнимателен, излишне самоуверен, склонен переоценивать свою значимость и игнорировать проблемы. Он сдержан в проявлении своих чувств, практичен и рассудителен, отличается радикализмом, то есть любит экспериментировать, открыт для чего-то нового, не склонен к бескомпромиссности, и у него высокий психологический возраст.
- *Техническая безграмотность.* Пользователь склонен срывать свою злость на других, у него высокий уровень интеллекта, он эмоционально нестабилен, все время находится в расслабленном состоянии, стремится контролировать любую значи-

мую ситуацию, считает, что его успехи обусловлены внешними обстоятельствами — удачей, везением. Такой человек не склонен считать себя ответственным за свои неуспехи и неудачи, он приписывает эту ответственность другим людям, также такой человек считает, что он легко завоевывает уважение других людей.

В зависимости от того, на какую из этих уязвимостей пользователя злоумышленник направляет свое атакующее воздействие, можно выделить различные варианты атакующих воздействий и ответные действия пользователя на них. В то же время особо стоит отметить, что ответные действия пользователей носят недетерминированный характер, то есть требуется переход к оценкам вероятности осуществления тех или иных ответных действий пользователя, а также, в конце концов, к вероятностным характеристикам успеха или неуспеха атаки, предпринятой злоумышленником.

Было рассмотрено несколько возможных, но не исчерпывающих вариантов атакующих воздействий и ответов (реакций пользователя) на них [9]. Очевидно, что определенное влияние злоумышленника на пользователя зачастую приводит к активации сразу нескольких уязвимостей.

Для перехода к оценкам вероятности ответных действий пользователей информационных систем был предложен следующий подход. Использовался ряд тестовых методик оценки степени выраженности психологических особенностей личности. На основании регрессионных уравнений, построенных по результатам исследования [19], по оценкам, полученным с помощью этих методик, вычислялись оценки степени выраженности уязвимостей пользователя. Исходя из полученных значений, была введена вероятностная мера оценки успеха социоинженерного атакующего воздействия злоумышленника, зависящая от степени проявления уязвимости пользователя. Определенный прогресс в построении математических моделей и расчетов оценок вероятности защищенности пользователей информационных систем от социоинженерных атак был представлен в [8]. В ходе работ также был найден подход к комбинации оценок вероятности успеха социоинженерных атакующих воздействий злоумышленника, в случае если при имитации социоинженерного атакующего воздействия было установлено, что атака может развиваться разными способами (путями), или, если при развитии атаки с близкими оценками вероятности могут быть использованы разные атакующие воздействия. Частным и достаточно понятным примером одной из возможных формул расчета комбинированной оценки вероятности успеха социоинженерного атакующего воздействия злоумышленника может служить:

$$p = 1 - (1 - p_1)(1 - p_2)(1 - p_3),$$

где p_1, p_2, p_3 — оценки вероятности успеха различных социоинженерных атакующих воздействий злоумышленника, а p — кумулятивная вероятность успеха злоумышленника.

3. ПРОГРАММНЫЙ МОДУЛЬ, ПРЕДНАЗНАЧЕННЫЙ ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ГРУПП ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Одной из важнейших подзадач задачи анализа защищенности пользователей информационных систем от социоинженерных атак является задача выделения групп пользователей по какому-либо признаку. Допустим, компания имеет распределенную структуру, и каждый офис имеет свой перечень конфиденциальных документов. В таком случае нецелесообразно проводить анализ защищенности всех пользователей

информационной системы, да еще и по-отдельности. Вместо этого, необходимо провести анализ защищенности группы пользователей, работающих в обособленном офисе. Более того, выделенная группа пользователей может обладать рядом специфических или особо выраженных уязвимостей. Поэтому в таком случае представляется обоснованным проводить анализ отдельно взятой группы пользователей с целью подготовки перечня мер по повышению уровня ее защищенности от социоинженерных атак. С целью выделения и анализа степени защищенности групп пользователей, был разработан программный модуль, предназначенный для использования в более широком комплексе программ, разработанном для анализа защищенности пользователей информационных систем от социоинженерных атак. Данный модуль также позволяет визуализировать контролируемые зоны информационной системы для наглядного представления структуры компьютерной сети компании и дифференциации пользователей по правам доступа к аппаратным средствам.

Данные об аппаратных средствах и пользователях, а также о связях между компонентами информационной системы извлекаются из базы данных, разработанной в рамках проекта по созданию прототипа комплекса программ для анализа защищённости пользователей информационных систем от социоинженерных атак.

Пользователю программного модуля доступны инструменты для визуализации отдельных контролируемых зон в виде графа, в котором вершинами являются аппаратные средства и пользователи информационной системы, а дугами – связи между ними. Визуально различимы вершины, соответствующие пользователям из различных групп, разделенных по правам доступа к информационным ресурсам.

Рассмотрим пример информационной системы, точнее ее модель, представленную на рис. 1.

В частности, с помощью данного программного модуля может быть сформирована графическая модель информационной системы. Пример такой модели представлен на рис. 1а. Также существует возможность выделения групп пользователей. Кроме того, с помощью данного программного модуля существует возможность имитации социоинженерного атакующего воздействия злоумышленника на выбранную группу пользователей информационной системы. Оператор может самостоятельно выбрать, на какого из пользователей будет совершено социоинженерное атакующее воздействие, какая конфиденциальная информация предположительно требуется злоумышленнику, а также задать ограничения на ресурсы злоумышленника.

После выполнения алгоритма имитации социоинженерного атакующего воздействия по заданным оператором параметрам выводится результат социоинженерного атакующего воздействия. Надпись «Задействовано 3 пользователя» означает, что конфиденциальная информация, требуемая злоумышленнику, найдена, а в ходе социоинженерной атаки злоумышленника им было скомпрометировано 3 пользователя информационной системы. Первым пользователем, который оказался сопряженным с злоумышленником при совершении последним социоинженерного атакующего воздействия, является пользователь с никнеймом «Иванова», далее по связям переходим к «Голубеву», информация была найдена на устройствах, доступных пользователю с никнеймом «Зайцев». Надпись «Успешность атаки от Иванова до Зайцев = 0,00014186» означает, что злоумышленник получит доступ к необходимой ему информации с вероятностью 0,00014186.

Кроме того, может быть выведено дерево атак, отражающее схему развития социоинженерной атаки злоумышленника. Также, для каждого пользователя информационной

системы можно из контекстного меню вызвать подробное описание уязвимостей и степень проявления этих уязвимостей (рис. 2).

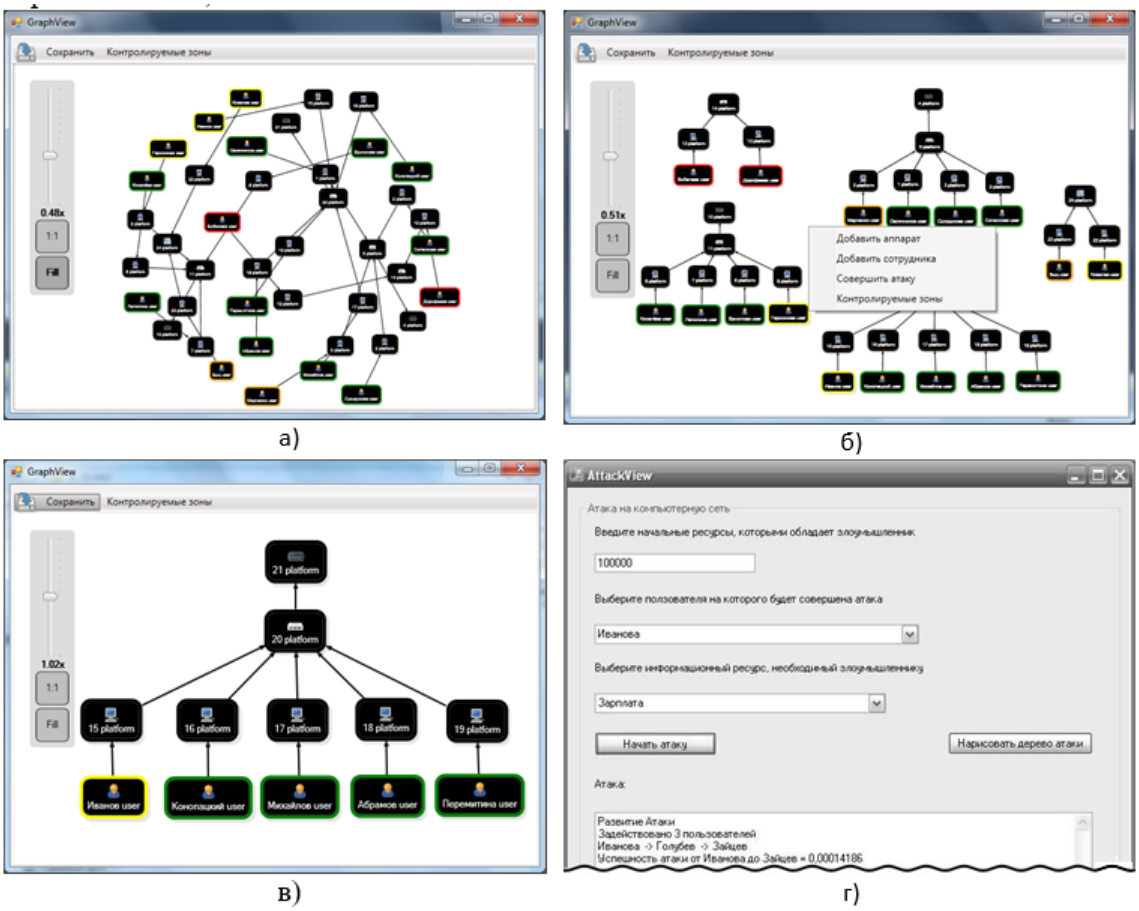

Рис. 1. Визуализация модели информационной системы, вывод результата имитации социоинженерного атакующего воздействия злоумышленника

Рис. 2. Степень проявления уязвимостей для пользователя «Голубев», дерево атак развития социоинженерной атаки злоумышленника

4. ЗАКЛЮЧЕНИЕ

В статье описан принцип построения оценки защищенности пользователя информационной системы по отношению к социоинженерным атакующим воздействиям злоумышленника. Рассматривались действия злоумышленника достаточно элементарного характера («одноходовки»), нацеленные на «элементарные» уязвимости пользователя, воздействие на которые приводит непосредственно к какому-то действию пользователя. Кроме того, в качестве иллюстрирующего примера использования предложенного принципа был представлен программный модуль, позволяющий проводить анализ защищенности групп пользователей информационных систем.

Полученные результаты могут быть использованы для обучения студентов по курсам «Информационная безопасность», в частности, в разделах, посвященных вопросам обеспечения безопасности пользователей информационных систем и защите конфиденциальных данных от инсайдерских атак. Кроме того, обсуждавшиеся проблемы служат источником заданий для лабораторных работ по теории графов и ее приложений, а также тем для курсовых и выпускных квалификационных работ.

Дальнейшие исследования в области лежат на стыке информатики, психологических и математических наук. В частности, требуют развития математические модели анализа защищенности пользователей информационных систем. Кроме того, предполагается принять в рассмотрение профиль компетенций злоумышленника для уточнения вероятностных оценок защищенности пользователей информационных систем. Наконец, с точки зрения формирования профиля уязвимостей пользователя, необходимо проводить дальнейшие исследования с целью выявления новых, не исключено, что более сложных, уязвимостей пользователей информационных систем.

Список литературы

1. Cox James Information systems user security: A structured model of the knowing–doing gap // Computers in Human Behavior. Sep2012. Vol. 28. Issue 5. P. 1849–1858.
2. CVSS. Common Vulnerability Scoring System. URL:www.first.org/cvss\T2A\cyre (дата обращения 13.08.2015).
3. *Jahyun Goo, Myung-Seong Yim, Dan J.* Kim IEEE 1. A path to successful management of employee security compliance: an empirical study of information security climate // Transactions on Professional Communication. Dec2014. Vol. 57. Issue 4. P. 286–308. 23p.
4. *Salvatore Distefanoa, Antonio Puliafitob.* Information dependability in distributed systems: The dependable distributed storage system // Integrated Computer-Aided Engineering 21 (2014). P. 3–18.
5. *Trcek Denis, Trobec Roman, Paveshich Nikola, Tasic J. F.* Information systems security and human behaviour // Behaviour & Information Technology. Mar-Apr 2007. Vol. 26. Issue 2. P. 113-–118.
6. *Zeadally Sherali, Yu Byunggu, Jeong Dong Hyun, Liang Lily.* Detecting insider threats: solutions and trends // Information Security Journal: A Global Perspective. 2012. Vol. 21. Issue 4. P. 183—192.
7. *Zhang Jianye, Zeng Qinshun, Song Yiyang, Li Cunbin.* Information security risk assessment of smart grid based on absorbing Markov chain and SPA // International Journal of Emerging Electric Power Systems 2014. 15(6). P. 527—532
8. *Азаров А.А.* Моделирование профиля уязвимостей пользователя в задачах оценки защищенности от социо-инженерных атак // Информационно-измерительные и управляющие системы. 2013. № 9, т. 11. С. 49–52.
9. *Азаров А.А., Тулупьева Т.В., Тулупьев А.Л.* Прототип комплекса программ для анализа защищенности персонала информационных систем, построенный на основе фрагмента профиля уязвимостей пользователя. // Труды СПИИРАН. 2012. Вып. 21. С. 21—40.

10. *Веденеев В.С., Бычков И.В.* Средства поиска инсайдеров в корпоративных ИС // Безопасность информационных технологий, 2014. № 1. С. 9—13.
11. Информационная безопасность бизнеса. Исследования текущих тенденций в области информационной безопасности бизнеса // Лаборатория Касперского. URL: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf (дата обращения: 30.04.2015)
12. *Котенко И.В., Степашкин М.В.* Системы-имитаторы: назначение, функции, архитектура и подход к реализации // Изв. вузов. Приборостроение. 2006. Т. 49, № 3. С. 3—8
13. *Котенко И.В., Юсупов Р.М.* Перспективные направления исследований в области компьютерной безопасности. Защита информации. Инсайд. 2006. № 2. С. 46.
14. Пентагон подсчитал, что Э. Сноуден похитил 1,7 млн секретных файлов // РБК / URL: http://top.rbc.ru/politics/10/01/2014/898589.shtml (дата обращения 01.03.2015)
15. Подросток рассказал, как была взломана почта директора ЦРУ // Вести / URL: http://hitech.vesti.ru/news/view/id/7905 (дата обращения 21.10.2015)
16. *Сапронов К.* Человеческий фактор и его роль в обеспечении информационной безопасности. URL: http://www.interface.ru/home.asp?artId=17137 (дата обращения 05.03.2015).
17. *Сергиевский М.* Сети — что это такое. // КомпьютерПресс, 1999, № 10. С. 3–9.
18. *Суворова А.В., Тулупьев А.Л., Пащенко А.Е., Тулупьева Т.В., Красносельских Т.В.* Анализ гранулярных данных и знаний в задачах исследования социально значимых видов поведения // Компьютерные инструменты в образовании, 2010. № 4. С. 30—38.
19. *Тулупьев А.Л., Тулупьева Т.В., Азаров А.А., Григорьева О.Ю.* Психологические особенности персонала, предрасполагающие к успешной реализации социо-инженерных атак // Научные труды Северо-Западного института управления РАНХиГС, 2012. Т. 3, вып. 3(7). С. 256–266.
20. Убытки от киберпреступлений продолжают расти // URL: http://www8.hp.com/ru/ru/software-solutions/ponemon-cyber-security-report/index.html (дата обращения 04.03.2015).

THE ANALYSIS OF THE INFORMATION SYSTEMS' USERS' GROUPS PROTECTION ANALYSIS FROM THE SOCIAL ENGINEERING ATTACKS: THE PRINCIPLE AND PROGRAM IMPLEMENTATION

Azarov A. A., Abramov M. V., Tulupyeva T. V., Tulupyev A. L.

Abstract

The actual task of users' protection analysis is to split the users of the information system into subgroups, for example, corresponding to the remote offices of the organization, and analysis of these subgroups of users. The article presents one of the modules of the software prototype that implements the users' of information systems protection analysis from socio-engineering attacks.

Keywords: *information security, social engineering attacks, users, information system, confidential data.*

Азаров Артур Александрович,
кандидат технических наук, старший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики (лаб. ТиМПИ) СПИИРАН; доцент кафедры информатики СПбГУ; старший научный сотрудник лаборатории информационных технологий в сфере социального компьютинга МПГУ,
artur-azarov@yandex.ru

Абрамов Максим Викторович,
младший научный сотрудник лаб. ТиМПИ СПИИРАН; младший научный сотрудник лаборатории информационных технологий в сфере социального компьютинга МПГУ; аспирант кафедры информатики СПбГУ
mva16@list.ru

Тулупьева Татьяна Валентиновна,
кандидат психологических наук, доцент, старший научный сотрудник лаб. ТиМПИ СПИИРАН; доцент кафедры информатики СПбГУ; доцент СЗИУ РАНХиГС,
tvt100a@mail.ru

Тулупьев Александр Львович,
доктор физико-математических наук, доцент, заведующий лаб. ТиМПИ СПИИРАН; профессор кафедры информатики СПбГУ,
alexander.tulupyev@gmail.com