

УДК 616.89

DOI: 10.17238/issn1998-5320.2020.14.2.20

Е. А. Калиберда¹, А. М. Шабалин²

¹Омский государственный технический университет, г. Омск, Российская Федерация

²Омская гуманитарная академия, г. Омск, Российская Федерация

Использование современных систем виртуализации для формирования профессиональных компетенций студентов вузов при изучении DLP-систем

Аннотация. Проблема и цель статьи: формирование профессиональных компетенций будущих специалистов в области защиты информации с помощью современных систем виртуализации. Методы: применение практико-ориентированного подхода как метода преподавания и обучения в сочетании с практической деятельностью, применение цифровых инновационных технологий виртуализации в качестве обязательной составляющей практико-ориентированного подхода. Для улучшения процесса формирования профессиональных компетенций, на основании полученной лицензии от компании InfoWatch, на базе Омского государственного технического университета была организована специализированная виртуальная лаборатория, позволяющая производить настройку и проверку DLP-системы, определять политику безопасности, обеспечивать контроль информационных потоков в компании, а также анализировать выявленные инциденты. Для этого был разработан алгоритм внедрения DLP-системы в учебный процесс, в котором студентами определяются объекты информационной безопасности и разрабатываются соответствующие политики для предотвращения утечки данных и выявления возможных инцидентов, осуществляются перехваты конфиденциальной информации по контролируемым каналам связи. Использование современных средств виртуализации при изучении функциональных возможностей современных DLP-систем позволяет студентам применить теоретические знания на практике и подготовиться к решению ряда профессиональных задач по обеспечению защищённости корпоративных организаций от внутренних утечек конфиденциальных данных.

Ключевые слова: практико-ориентированные технологии, цифровые технологии в образовании, сформированность профессиональных компетенций, информационная безопасность, внутренние угрозы, DLP-система, InfoWatch, виртуальная лаборатория

Дата поступления статьи: 11 февраля 2020 г.

Для цитирования: Калиберда Е. А., Шабалин А. М. (2020). Использование современных систем виртуализации для формирования профессиональных компетенций студентов вузов при изучении DLP-систем // Наука о человеке: гуманитарные исследования. Т. 14. № 2. С. 118–122. DOI: 10.17238/issn1998-5320.2020.14.2.20

Проблема и цель. В современном образовании с недавнего времени появилось такое понятие, как *skills*, обозначающее базовые навыки или профессиональные компетенции выпускника, которые можно разделить на *hard* (жесткие) и *soft* (мягкие) [1]. Первые указывают на знание профессии, вторые – на умение работать в коллективе, общаться, презентовать свои наработки и т. д. Оба типа компетенций, безусловно, важны для выпускника вуза, и тем не менее относительно недавно специалисты заговорили о необходимости еще и *digital skills* – наборе цифровых навыков, которые нужны современным специалистам в рамках работы в сетевой цифровой экономике [2].

Цифровая парадигма образования, в том числе высшего, рассматривается в разных контекстах, но развитие *digital skills* – это ключевой момент в подготовке на разных уровнях образования, позволяющий готовить полноценного члена общества, готового работать с сетевыми цифровыми технологиями, которые приносит в современную экономику XXI век [3–6].

Digital skills могут рассматриваться в зависимости от направления обучения как *hard skills*, если эти навыки являются профессиональными для студента, или *soft skills*, если они рассматриваются с точки зрения общеобразовательных компетенций.

Информационная безопасность, на наш взгляд, относится именно к такой сфере профессиональной деятельности, так

как навыки безопасной работы с информацией должны быть у всех, как у специалистов, так и у рядовых пользователей, деятельность которых напрямую не связана с информационной безопасностью. Для специалистов в области информационной безопасности умения противостоять внутренним и внешним угрозам – это, несомненно, *hard skills*; для других же специальностей информационная безопасность рассматривается как *soft skills*, так как «небезопасникам» не нужно понимать все тонкости борьбы с вредоносным программным обеспечением, но они должны быть грамотными в области информационной безопасности, знать её основы, понимая, что можно сделать в определённых ситуациях, чтобы сохранить конфиденциальность, целостность и доступность важной информации.

В данной статье сделан упор на подготовку специалистов в области информационной безопасности, а значит, *digital skills* здесь рассматриваются на профессиональном уровне *hard skills*.

Одно из главных требований, которое предъявляется к современному специалисту по защите информации, – это умение решать реальные задачи информационной безопасности бизнес-процессов и менеджмента организации [7]. Информационная безопасность, «оторванная» от бизнеса, сегодня никому не нужна.

Это, в свою очередь, определяет необходимость повышения практической ориентированности специалистов по защите информации, то есть развития широкого набора профессиональных компетенций, позволяющих выпускникам направления «Информационная безопасность» быстро включаться в деятельность организации работодателя и применять знания в решении актуальных задач сохранения конфиденциальной информации.

Так, с 2017 года при подготовке специалистов в области защиты информации стали появляться рекомендации о развитии у студентов профессиональной компетенции под названием «Корпоративная защита от внутренних угроз информационной безопасности», которая направлена на защиту от внутренних утечек данных, произошедших умышленно или по неосторожности через технические каналы связи. Студенты должны знать основы противодействия от данному типу угроз, уметь применять нормативно-правовые акты при расследовании инцидентов, уметь использовать системы и методы, предназначенные для защиты данных [8].

С точки зрения digital skills будущие специалисты в области информационной безопасности должны уметь работать с современными программными комплексами, обеспечивающими защиту корпоративной информации от внутренних утечек. Такие комплексы называются DLP-системами (Data Loss Prevention).

Подготовка студентов по работе с современными DLP-системами – технически сложный процесс, успешно организовать и провести который можно только, на наш взгляд, в специально оборудованной виртуальной вузовской лаборатории [9]. Такая лаборатория вот уже два года эффективно функционирует в Омском государственном техническом университете (ОмГТУ) и помогает решить целый ряд образовательных задач при преподавании различных информационных дисциплин. Однако важнейшее значение она приобрела

после профилизации её для изучения функциональных возможностей современных DLP-систем.

Методы. В качестве методологической базы исследования выступил компетентностный подход. Исследование проводилось в ОмГТУ с привлечением студентов направления подготовки «Информационная безопасность». В работе использовались теоретические методы (сравнение, анализ, обобщение, конкретизация, моделирование) и эмпирические методы (педагогический эксперимент, анализ результатов деятельности). Основу исследования составили научные положения об организации практико-ориентированного обучения. Без применения практико-ориентированных технологий при подготовке специалистов в области защиты информации решение задачи подготовки конкурентоспособного специалиста представляется достаточно проблематичным.

Авторы работы [10] в своей статье говорят о том, что, только объединяя теорию и практику, студенты (которым обычно не хватает реального опыта работы) могут понять некоторые абстрактные понятия и принципы, сформулированные в теоретическом курсе. В работе [11] говорится о повышении мотивации у студентов в результате внедрения в процесс обучения лабораторных виртуальных стендов, способствующих формированию практических навыков у обучающихся.

Применение современных средств виртуализации в учебном процессе позволяет значительно укрепить связь студентов с изучаемой ими дисциплиной и улучшить понимание данного предмета в целом.

Выпускник высшего учебного заведения должен уметь решать сложные профессиональные задачи, поэтому формирование цифровых компетенций, безусловно, является для него обязательным и необходимым. Внедрение инновационных цифровых технологий делает доступным интерактивное взаимодействие в виртуальном формате, которое тесно связано с индивидуальным обучением [12].

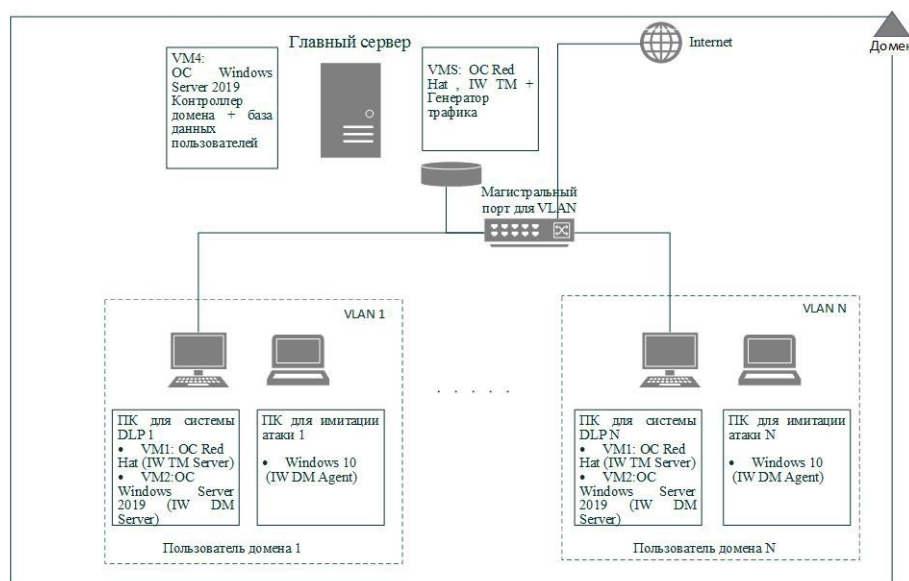


Рис. 1. Схема работы виртуальной лаборатории InfoWatch

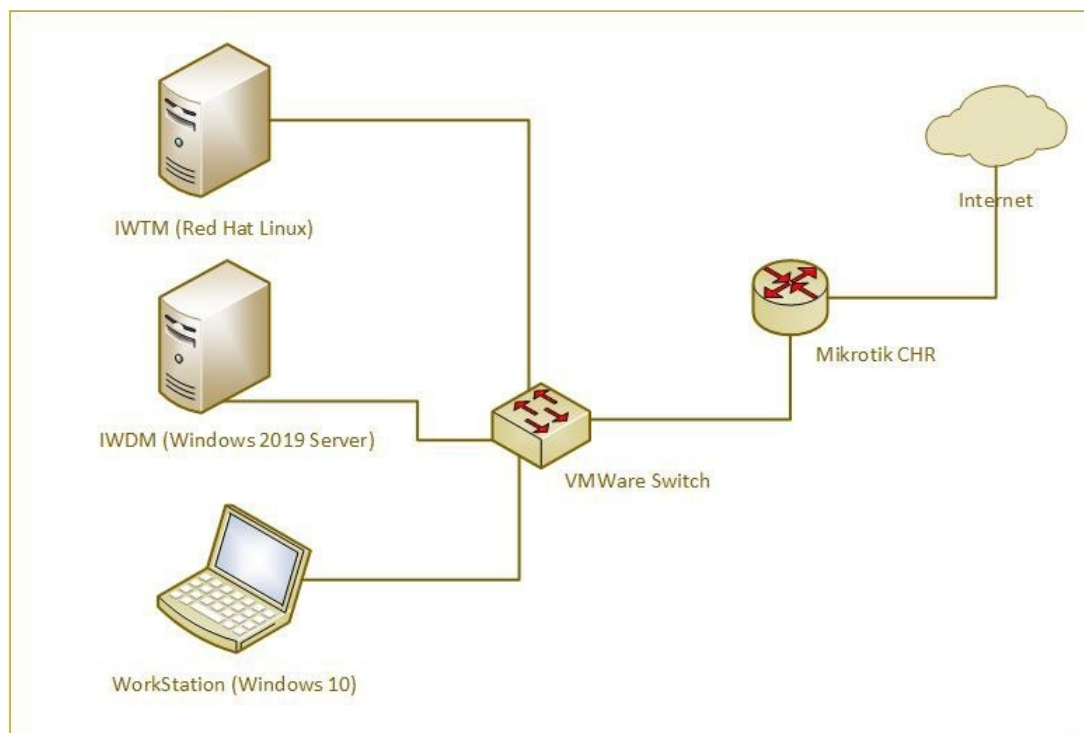


Рис. 2. Логическая топология рабочего места студента

Результаты. Для работы с современными DLP-системами, а также с целью внедрения практико-ориентированных технологий профессиональной подготовки в виртуальной лаборатории ОмГТУ были организованы специализированные стенды, где с помощью современных программных средств студенты производят настройку и проверку DLP-системы, определяют политики безопасности, обеспечивают контроль информационных потоков в компании и анализируют выявленные инциденты. В качестве средства обучения был выбран программный продукт Traffic Monitor 6 российской компании InfoWatch. Принцип работы виртуальной лаборатории представлен на рисунке 1.

Данная виртуальная инфраструктура реализуется с помощью гипервизора VMWare ESXi Server 6.5, средствами которого у каждого студента создаётся свой виртуальный стенд. Топология рабочего места студента представлена на рисунке 2.

Каждое виртуальное рабочее место студента состоит из двух серверов InfoWatch Traffic Monitor (IWTM, IWDM), а также компьютера сотрудника, с которого возможно эмулировать подозрительную активность в сети организации.

Работа в данной виртуальной лаборатории способствует организации практической подготовки студентов и формированию их профессиональных компетенций. При апробации работы стендов студентами в качестве объекта корпоративной защиты от внутренних угроз информационной безопасности рассматриваются гипотетические компании.

Для минимизации ложных срабатываний DLP-системы в сети организации следует чётко соблюдать определённый порядок действий. Алгоритм внедрения, разработанный авторами статьи (см. рис. 3), содержит четыре последовательных этапа:

1. Предпроектное исследование;
2. Установка DLP-системы;
3. Ввод в опытную эксплуатацию;
4. Ввод в промышленную эксплуатацию.

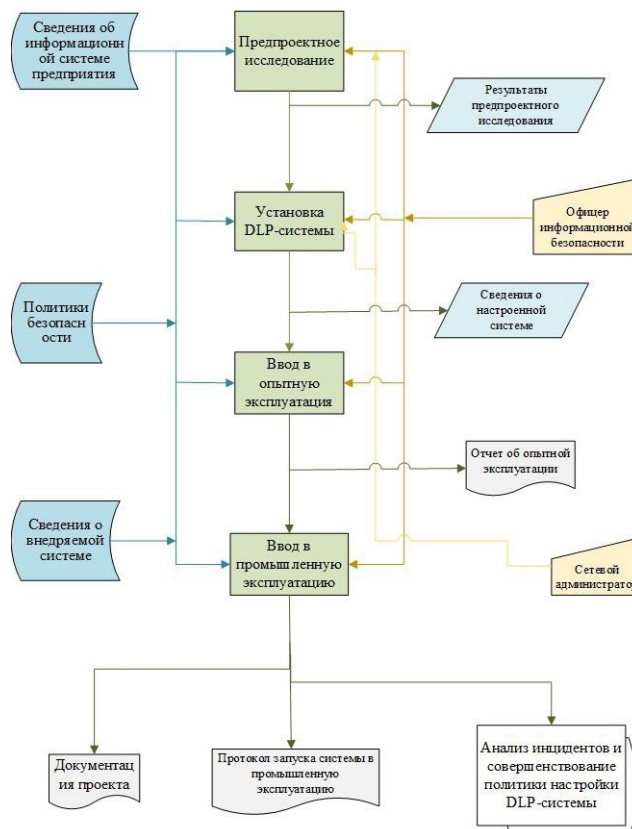


Рис. 3. Основные этапы внедрения DLP-системы, реализуемые студентами в виртуальной лаборатории

Все процессы перечисленных этапов реализуются студентами на лабораторных работах.

Моделирование ситуации, максимально приближенной к реальной профессиональной деятельности, позволяет существенно сократить или преодолеть разрыв между учебным и производственным процессом, а значит, сформировать необходимые профессиональные компетенции.

В результате теоретических и практических действий в соответствии с предлагаемым алгоритмом студенты в течение семестра создают проект качественно функционирующей DLP-системы. На виртуальном стенде ими разрабатываются и апробируются многочисленные политики безопасности для гипотетической организации. Например, студент определяет конфиденциальную информацию внутри компании и выделяет её отличительные признаки (эталонный документ, график, печать, ключевые слова и т. д.).

После разработки политик безопасности студенты проводят перехваты конфиденциальной информации. Например, имитируется отправка некоего конфиденциального документа по электронной почте, но система должна не допустить этого, выделив некоторые определённые студентом признаки конфиденциальности: наличие печати, ключевых слов и т. д. Также на клиентском компьютере им определяется список внешних устройств, с которыми можно работать пользовате-

лю, и отключается не разрешённое для использования в рабочее время программное обеспечение.

На завершающем этапе работы обучаемые используют аналитический функционал DLP-системы для создания отчётов о выявленных инцидентах и анализа полученных данных.

Следовательно, на созданных виртуальных стендах лаборатории студентами поэтапно проводятся различные подготавливающие работы, которые позволяют сформировать набор умений и определить алгоритм работы в различных критических ситуациях, максимально приближенных к практической деятельности.

Выводы. В результате работы в виртуальной лаборатории студенты успешно развивают профессиональную компетенцию «Корпоративная защита от внутренних угроз информационной безопасности»: ими апробируется функционал современных DLP-систем. Для гипотетической организации они выявляют актуальные внутренние угрозы и каналы утечек, определяют конфиденциальную информацию и этапы внедрения DLP-системы в работу компании. Таким образом, использование современных систем виртуализации при изучении DLP-систем является, на наш взгляд, обязательной составляющей образовательного процесса в вузе, которая позволяет сформировать профессиональные компетенции будущих специалистов в области защиты информации.

Источники

1. Галажинский Э. Чему не учат в университетах [Электронный ресурс] // Вестник, 2017, 2 августа, URL: <https://www.vedomosti.ru/opinion/articles/2017/08/03/727760-ne-uchat-v-universitetah> (дата обращения 02.03.2020).
2. Попова О. И. Трансформация высшего образования в условиях цифровой экономики // Вопросы управления. 2018. № 5 (35). С. 158–160.
3. Подольский О. Какими цифровыми компетенциями должны обладать кадры будущего? [Электронный ресурс] // Национальная техническая инициатива, 2020, 3 февраля, URL: <https://ntinews.ru/blog/publications/kakimi-tsifrovymi-kompetentsiyami-dolzny-obladat-kadry-budushchego-.html> (дата обращения 02.03.2020).
4. Istvan Simonic, Digital competency in higher education. 2013 International Conference on Interactive Collaborative Learning (ICL), 2013, pp. 88–91.
5. Тульчинский Г. В. Цифровая трансформация образования, вызовы для высшей школы // Российский журнал философских наук. 2017. № 6, С. 121–136.
6. Gaivoronkii D. V., Kutuzov V. M., Minina A. A. Digital transformation of engineering education. Strategic Partnership of Universities and Enterprises of Hi-Tech Branches (Science. Education. Innovations), 2017, pp. 3–6. DOI: 10.1109/TVForum.2017.8245954
7. Вайндорф-Сысоева М. Е., Субочева М. Л. «Цифровое образование» как системообразующая категория: подходы к определению // Вестник Московского государственного областного университета. Серия: Педагогика. 2018. № 3. С. 25–36.
8. Информационная безопасность корпорации: актуальная компетенция Digital Skills [Электронный ресурс]. URL: <https://worldskills.ru/media-czentr/novosti/informacionnaya-bezopasnost-korporaczii-aktualnaya-kompetenciya-digitalskills.html> (дата обращения: 02.03.2020).
9. Шабалин А. М., Калиберда Е. А. Построение виртуальной модели защиты корпоративной информации с использованием системы Infowatch Traffic Monitor // Вестник кибернетики. 2020. № 1 (37). С. 35–42.
10. Huang Shihong; Distant D. On Practice-Oriented Software Engineering Education Software, Engineering Education and Training Workshops (CSEETW), 2006, pp. 15–15. DOI: 10.1109/CSEETW.2006.11
11. Julien Broisin, Rémi Venant, Philippe Vidal All Authors A remote laboratory to leverage motivation of learners to practice: An exploratory study about system administration, Proceedings of 2015 12th International Conference on Remote Engineering and Virtual Instrumentation (REV), 2015, pp. 140–142. DOI: 10.1109/REV.2015.7087280
12. Li Bian Application of Digital Technology in Open and Distance Education, 2009 International Conference on Networking and Digital Society, 2009 (5), pp. 273–276. DOI: 10.1109/ICNDS.2009.74

Информация об авторах

Калиберда Елена Анатольевна

Кандидат технических наук, доцент кафедры «Математические методы и информационные технологии в экономике». Омский государственный технический университет (644050, РФ, г. Омск, пр. Мира, 11). ORCID ID: <https://orcid.org/0000-0003-2331-7572>, Scopus ID: 57201735193. E-mail: elekaliberda@rambler.ru

Шабалин Андрей Михайлович

Кандидат педагогических наук, доцент кафедры информатики, математики и естественнонаучных дисциплин. Омская гуманитарная академия (644105, РФ, г. Омск, ул. 4-я Челюскинцев, 2а). ORCID ID: <https://orcid.org/0000-0003-2404-9864>, Scopus ID: 57201738822. E-mail: sham.omsk@gmail.com

E. A. Kaliberda¹, A. M. Shabalin²

¹Omsk State Technical University, Omsk, Russian Federation

²Omsk Humanitarian Academy, Omsk, Russian Federation

The impact of modern virtualization systems on university students' professional competences while studying DLP systems

Abstract. The problem and purpose of the article is to shape professional competencies of future specialists in the information security field using modern virtualization systems.

The use of a practice-based approach as a method of teaching and learning in combination with practical activities. The use of digital innovative virtualization technologies as a mandatory component of a practice-based approach.

To improve the process of shaping professional competencies, (on the basis of a license from InfoWatch) a specialized virtual laboratory was organized on the basis of the Omsk State Technical University; it allowed configuring and verifying the DLP system, determining security policies, ensuring control of information flows in the company and analyzing identified incidents. For this purpose, an algorithm for introducing a DLP system into the educational process have been developed, the students could define information security objects and develop appropriate policies to prevent data leakage and identify possible incidents, intercepts confidential information through controlled communication channels.

The use of modern virtualization tools for studying the functionality of modern DLP systems allows students to put theoretical knowledge into practice and be ready to solve different professional tasks ensuring the corporate organizations protection from internal leakage of confidential data.

Keywords: practice-oriented technologies, digital technologists in education, shaping professional competencies, information security, internal threats, DLP system, InfoWatch, virtual laboratory.

Paper submitted: February 11, 2020

For citation: Kaliberda E. A., Shabalin A. M. (2020). The impact of modern virtualization systems on university students' professional competences while studying DLP systems. The Science of Person: Humanitarian Researches, vol. 14, no. 2, pp. 118–122. DOI: 10.17238/issn1998-5320.2020.14.2.20.

References

- Galazhinsky E. The things Universities do not teach [Electronic resource]. Vedomosti, 2017, August 2, URL: <https://www.vedomosti.ru/opinion/articles/2017/08/03/727760-ne-uchat-v-universitetah> (accessed 02.03.2020). (In Russian).
- Popova O. I. Transformation of higher education in the conditions of the digital economy. Management Issues . 2018, no. 5 (35). pp. 158–160. (In Russian).
- Podolsky O. What digital competencies should the staff of the future have? [Electronic resource]. National Technical Initiative, 2020, February 3, URL: <https://ntinews.ru/blog/publications/kakimi-tsifrovymi-kompetentsiyami-dolzhen-obladat-kadry-budushchego-.html> (accessed 02.03.2020). (In Russian).
- Istvan Simonics, Digital competency in higher education. 2013 International Conference on Interactive Collaborative Learning (ICL), 2013, pp. 88–91.
- Tulchinsky G. Digital Transformation of Education, Challenges for Higher School, Russian Journal of Philosophical Sciences. no. 6. 2017, pp. 121–136. (In Russian).
- Gaivoronskii D. V., Kutuzov V. M., Minina A. A. Digital transformation of engineering education. Strategic Partnership of Universities and Enterprises of Hi-Tech Branches (Science. Education. Innovations), 2017, pp. 3–6. DOI: 10.1109/IVForum.2017.8245954
- Vayndorf-Sysoeva M. E., Subocheva M. L. "Digital education" as a backbone category: approaches to definition. Bulletin of Moscow State Regional University. Series: Pedagogy. 2018, no. 3. pp. 25–36. (In Russian).
- Information security of the corporation: the current competency of Digital Skills [Electronic resource]. URL: <https://worldskills.ru/media-centr/novosti/informacionnaya-bezopasnost-korporaczii-aktualnaya-kompetenciya-digitalskills.html> (accessed 02.03.2020). (In Russian).
- Shabalin A. M., Kaliberda E. A. Building a virtual model for protecting corporate information using the Infowatch Traffic Monitor system. Bulletin of Cybernetics. 2020, no. 1 (37), pp. 35–42. (In Russian).
- Huang Shihong; Distant D. On Practice-Oriented Software Engineering Education Software, Engineering Education and Training Workshops (CSEETW), 2006, pp. 15–15. DOI: 10.1109/CSEETW.2006.11
- Julien Broisin, Rémi Venant, Philippe Vidal All Authors A remote laboratory to leverage motivation of learners to practice: An exploratory study about system administration. Proceedings of 2015 12th International Conference on Remote Engineering and Virtual Instrumentation (REV), 2015, pp. 140–142. DOI: 10.1109/REV.2015.7087280
- Li Bian Application of Digital Technology in Open and Distance Education, 2009 International Conference on Networking and Digital Society, 2009 (5), pp. 273–276. DOI: 10.1109/ICNDS.2009.74.

Information about the authors

Elena A. Kaliberda

Cand. Sc. (Engineering), Associate Professor. Omsk State Technical University (11 Mira Ave., Omsk, 644080, Russian Federation).

E-mail: elekaliberda@rambler.ru

Andrey M. Shabalin

Cand. Sc. (Pedagogy), Associate Professor. Omsk Humanitarian Academy (2a 4th Cheluskintsev st., Omsk, 644105, Russian Federation).

E-mail: sham.omsk@gmail.com

© E. A. Калиберда, А. М. Шабалин, 2020