УДК 378.1:004

ОПЫТ МИГРАЦИИ ЯДРА АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ С OPENLDAP И KERBEROS НА SAMBA

А.В. Соловьев

EXPERIENCE OF MIGRATION OF THE AUTHENTICATION AND AUTHORIZATION ENGINE OF INFORMATION AND EDUCATIONAL ENVIRONMENT FROM OPENLDAP AND KERBEROS TO SAMBA

A.V. Soloviev

Аннотация. В статье описана разработанная ранее и обновленная в 2020 г. архитектура Комплекса многоплановой поддержки образовательного процесса (КОМПОТ), состоящего из ядра авторизации и аутентификации (A&A), DNS-служб, почтовой системы, различных веб-сервисов, а также служб удалённого доступа (SSH и Windows Terminal-сервер). При обновлении Windows Terminal-сервера комплекса потребовались изменения в конфигурации ядра A&A. Вместо отдельных служб OpenLDAP и Kerberos применена служба Samba. Также описаны сопутствующие изменения в почтовой системе и DNS-службах. В результате сократилось число служебных компонентов комплекса. Совместно с внедрением платформы виртуализации Proxmox VE ряд компонентов было изолировано на отдельных виртуальных машинах. Всё это привело к упрощению администрирования и повышению информационной безопасности.

Ключевые слова: *аутентификация и авторизация; OpenLDAP; Kerberos; Samba; OpenAFS; информационно-образовательная среда.*

Abstract: The article describes the structure of the Complex of versatile support for the educational process (KOMPOT) developed earlier and updated in 2020. The complex contains the authorization and authentication (A&A) engine, DNS services, the mail system, various web services, as well as remote access services (SSH and Windows Terminal Server). Update of Windows Terminal Server required changes in configuration of the A&A engine of the complex. Integrated Samba service was introduced instead of separate OpenLDAP and Kerberos services. Also the article describes some related changes to the mail system and DNS services. As a result, the number of auxiliary components of the complex was reduced. Introduction of the Proxmox Virtualization Environment allows a number of components to be isolated on separate virtual machines. All this has led to simplified administration and increased information security.

Key words: *authentication and authorization, OpenLDAP, Kerberos, Samba, OpenAFS, information and educational environment.*

Введение

Информационно-образовательная среда (ИОС) КОМПОТ – Комплекс многоплановой поддержки образовательного процесса – разработан студентами и сотрудниками кафедры информационно-измерительных систем и физической электроники в 2006 г. и уже более 13 лет успешно применяется в физико-техническом институте (ФТИ) ПетрГУ [1, 2]. К задачам комплекса относится централизованная авторизация и аутентификация (A&A) пользователей, предоставление файлового хранилища, организация системы электронной почты, а также реализованные в виде веб-сервисов различные функции по текущему учёту успеваемости и прочих достижений студентов. За исключением Windows Terminal-сервера, комплекс составлен из компонентов, являющихся свободным программным обеспечением.

КОМПОТ – не единственная ИОС, используемая в ПетрГУ. Основные административно-управленческие задачи решаются ИАИС (Информационно-аналитической интегрированной системой), также разработанной в ПетрГУ [3], в качестве виртуальных обучающих сред используются такие универсальные продукты, как Moodle, BlackBoard, WebCT [4] и проч. От этих систем КОМПОТ отличается возможностью аутентифицировать и авторизовать пользователя на компьютерах общего доступа (в дисплейных классах) и предоставить ему сетевой доступ к его персональному файловому хранилищу.

За годы использования комплекса приходилось решать различные технические задачи по его развитию и обновлению. В данной работе описаны проблемы, возникшие при обновлении Windows Terminal-сервера удалённого доступа, интегрированного в комплекс, потребовавшие переконфигурирования ядра A&A.

Работа состоит из двух частей и заключения. В первой части описана структура первой версии конфигурации комплекса 2006–2019 гг. В первую очередь уделено внимание взаимодействию сервисов A&A с остальными модулями комплекса. Вторая часть посвящена описанию модифицированной в 2020 г. конфигурации комплекса, адаптированной под новые требования. В заключении обсуждаются особенности изменённой конфигурации.

Описание первой версии комплекса

В ходе разработки комплекса среди различных распределённых сетевых файловых систем предпочтение было отдано AFS в реализации OpenAFS, как наиболее приспособленной для существования под разными операционными системами [5]. Исходя из требований OpenAFS были выбраны протоколы для A&A. Структурная схема комплекса представлена на рис. 1. Отдельные хосты с сервисами обозначены на рисунке пунктирными рамками (KOMPOT, JUPITER, MARS, IQ,…).

Ядром КОМПОТ является централизованная система A&A на основе протоколов LDAP (в реализации OpenLDAP) и Kerberos 5 (в реализации Heimdal KDC). Служба каталогов LDAP позволяет хранить разнообразную учётную информацию о студентах и сотрудниках института, их роли и права доступа, а Kerberos-сервер обеспечивает безопасную и надёжную аутентификацию клиентов. Ядро A&A используется многочисленными модулями, составляющими комплекс.

Также на основе пакетов DJB DNS (tinydns и dnscache) КОМПОТ обеспечивает поддержку доменной зоны для нужд ФТИ.

Протокол Kerberos является необходимым средством аутентификации в сетевой распределённой файловой системе OpenAFS, используемой для хранения томов пользователей; поддерживается через прослойку SASL в почтовом сервисе Cyrus; в веб-сервере Apache поддерживается через модуль аутентификации mod_auth_kerb, благодаря чему централизованная A&A внедрена в различные веб-сервисы комплекса: веб-сервис онлайн-тестирования знаний iq.karelia.ru [6], веб-сервис учёта посещаемости и успеваемости студентов «Кондуиты» [7], веб-сервис «Система учёта публикаций» [8] и проч.

На компьютерах в дисплейных классах с Linux (в разное время использовались различные версии дистрибьютивов Debian от Sarge в 2006 г. до Buster в наст. время) авторизация пользователей реализована через механизмы PAM (модули pam_krb5 и pam_afs_session) и NSS (модуль libnss-ldapd). Такая же конфигурация на SSH-шлюзе комплекса MARS, обеспечивающем пользователям удалённый доступ к своему файловому тому, а также на SSH-шлюзе SATURN, предоставляющем доступ к вычислительному кластеру ФТИ «Лусидору» [9].

Интегрированная с ядром A&A служба Samba реализует контроллер домена для сети Microsoft, обеспечивая авторизацию пользователей на Windows Terminal-сервере JUPITER. Согласованность баз данных LDAP, OpenAFS, Kerberos и Samba реализована при помощи разработанных специально для данного комплекса сценариев административного веб-сервиса на языке PHP.

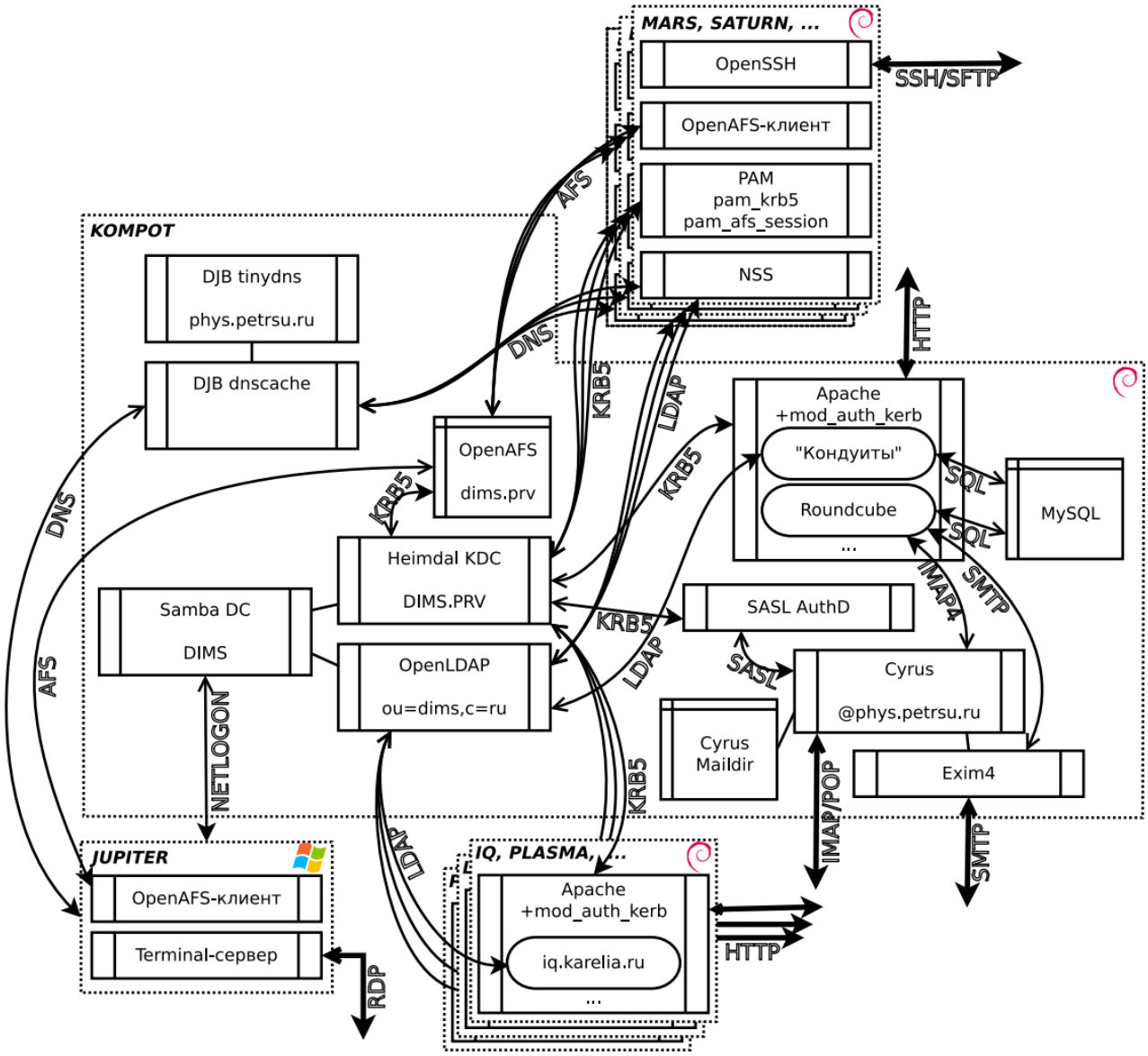

Рисунок 1 — Структурная схема КОМПОТ, версия 1 (2006–2019 гг.), заполненное острие соединительной линий обозначает клиентскую сторону взаимодействия, а контурное острие – серверную, утолщённые линии – внешние интерфейсы системы

Службы ядра комплекса запущены на хосте KOMPOT под управлением Debian GNU/Linux 10 «Buster» на сервере Kraftway GEG Express 100 (2 ЦПУ Intel Xeon E5410 3.00 ГГц, ОЗУ 12 Гб), аналогичное аппаратное обеспечение используется для Windows Terminal-сервера JUPITER под управлением Microsoft Windows Server 2003.

Резервное копирование выполняется периодически на не показанное на рис. 1 внешнее сетевое хранилище по протоколам NFS и SMB/CIFS.

Модификация конфигурации комплекса

Все компоненты комплекса, кроме Windows Terminal-сервера, основаны на свободном программном обеспечении, поэтому обновление отдельных компонентов происходило без каких-либо серьёзных переделок в конфигурации. К сожалению, в 2010 г. компания Microsoft прекратила поддержку Windows Server 2003 (а в 2015 г. – и расширенную поддержку), из-за чего обновление программного обеспечения на Windows Terminal-сервере становится невозможным. Новые версии Windows Server не поддерживают технику

авторизации на основе контроллера домена и требуют для этой цели службу Active Directory (AD). С учётом этого требования в 2020 г. конфигурация комплекса была изменена.

В новом варианте конфигурации комплекса (рис. 2) ядро A&A реализовано на основе сервиса Samba 4 в режиме совместимости с AD. В этом режиме служба Samba представляет собой интегрированный сервис на основе протоколов LDAP, Kerberos и DNS со специфическими для AD расширениями, что привело, в свою очередь, к следующим изменениям.

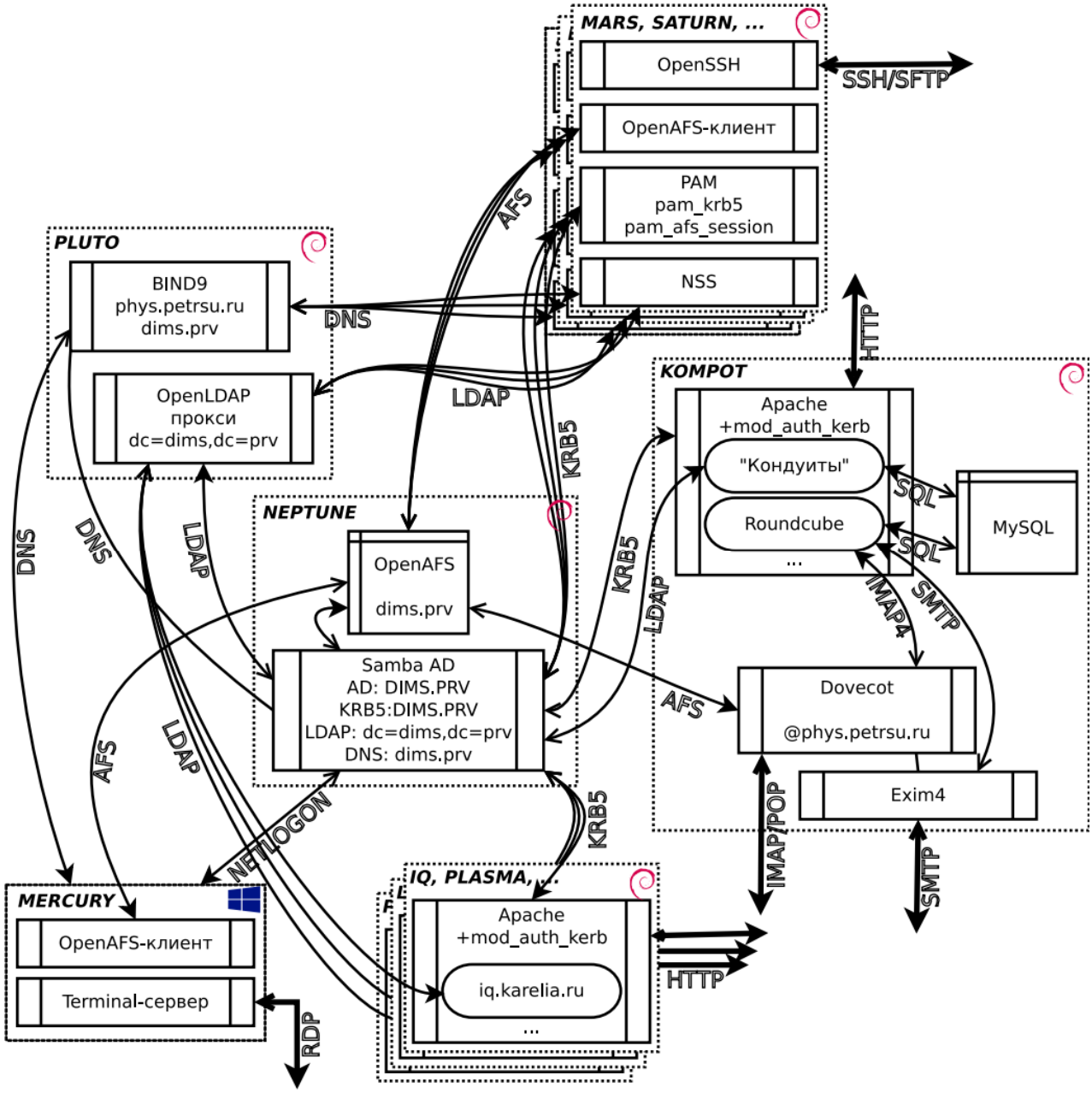

Рисунок 2 — Структурная схема КОМПОТ, версия 2 (2020 г.)

Используемая ранее служба OpenLDAP предоставляла возможность гибко конфигурировать доступ к различным атрибутам каталога LDAP. Реализация AD в Samba не предоставляет такой возможности: аутентифицированный пользователь имеет доступ к любым атрибутам. Поэтому существенные персональные данные пользователей из LDAP были перенесены в изолированную базу данных MySQL. Эти данные используются в веб-сервисе «Кондуиты» и для администрирования комплекса, поэтому такая переделка не повлияла на другие компоненты.

ISSN 2413–9858

Также был добавлен анонимный LDAP-прокси сервис на основе OpenLDAP, предоставляющий минимально необходимую информацию для модулей libnss-ldapd на клиентских Linux-машинах. Это избавляет от необходимости хранить на каждой рабочей станции Linux учётные данные служебного пользователя, обеспечивающего доступ к AD-LDAP.

Встроенная в AD служба DNS непригодна для произвольных изменений доменной зоны, поэтому отдельный DNS-сервер для нужд ФТИ ПетрГУ по-прежнему востребован. Однако было решено заменить связку DJB tinydns + dnscache (которая за годы эксплуатации вызывала некоторые нарекания по стабильности работы) на сервер BIND9, настроенный для трёх функций: как авторитетный DNS-сервер – для домена ФТИ ПетрГУ, как рекурсивный и кэширующий DNS-сервер – для клиентов в сети ПетрГУ и как перенаправляющий – для домена AD.

Переключение с Heimdal KDC на Samba AD Kerberos прошло без изменений в конфигурации комплекса.

В ходе модификации комплекса было решено отказаться от почтовой системы Cyrus. Она хранит почтовые сообщения в собственном хранилище, что усложняет администрирование системы в части назначения пользователям квот и выполнения резервного копирования. Существующий агент передачи почты (MTA) Exim 4 был перенастроен с доставки по LMTP в Cyrus на доставку при помощи Dovecot с сохранением почты в формате Maildir в персональном томе пользователя в OpenAFS. В результате почтовая квота пользователя стала частью его файловой квоты и пропала необходимость в отдельном резервном копировании почтового хранилища, поскольку оно совмещено с файловым.

BIND9 и OpenLDAP не могут работать на одном сетевом интерфейсе с службой Samba AD, поэтому эти службы были разнесены по разным хостам. Следует отметить, что такое изолирование сервисов повышает информационную безопасность комплекса в целом.

Обновлённая конфигурация комплекса реализована в виде нескольких виртуальных машин на основе платформы виртуализации Proxmox VE 6.3, запущенных на сервере Тринити C950458 (2 ЦПУ Intel Xeon E5-2630v4 2.2 ГГц, ОЗУ 64 Гб): виртуальная машина NEPTUNE (4 виртуальных ЦПУ, 2 Гб виртуального ОЗУ) под Debian GNU/Linux 10 «Buster», виртуальная машина MERCURY (30 виртуальных ЦПУ, 40 Гб виртуального ОЗУ) под Microsoft Windows Server 2012 R2 (с функцией Terminal-сервера) и виртуальный Linux-контейнер (LXC) PLUTO (2 виртуальных ЦПУ, 2 Гб виртуального ОЗУ). Почтовая система и веб-сервисы остались на «старом» хосте KOMPOT.

Заключение

В результате обновления программного и аппаратного обеспечения комплекса удалось сократить количество критически важных компонентов: вместо трёх отдельных служб Heimdal KDC, OpenLDAP и Samba DC, которые требовали принудительного обеспечения согласованности, внедрена служба Samba AD с OpenLDAP-прокси; вместо отдельных служб tinydns и dnscache – единственная служба BIND9; замена Cyrus на Dovecot позволила упростить администрирование почтовой системы. Несмотря на дробление служб комплекса по отдельным хостам благодаря виртуализации администрирование системы в целом не усложнилось, зато удалось повысить её информационную безопасность. Комплекс построен на основе свободного программного обеспечения (за исключением Terminal-сервера), что позволяет гибко манипулировать его конфигурацией, модифицируя её под нужды пользователей, и, при необходимости, тиражировать.

ЛИТЕРАТУРА

1. Ершова Н. Ю., Назаров А. И., Соловьев А. В. Практика организации учебного процесса с применением специализированных средств сетевого обучения // Материалы V Международной научно-практической конференции «Электронная Казань–2013», 2013. Вып. № 1(11), ч. II. С. 58–64.

2. Мощевикин А. П., Соловьев А. В. Web-сервис учёта посещаемости и успеваемости «Кондуиты» // Материалы научно-методической конференции «Университеты в образовательном пространстве региона: опыт, традиции и инновации» (21–23 ноября 2007 г.). Петрозаводск : Изд-во ПетрГУ, 2007. Ч. II (Л-Я). С. 117–118.

3. Информационно-аналитическая интегрированная система ПетрГУ: подходы, решения, направления развития / С.Х. Костюкевич и др. // Университетское управление: практика и анализ, 2015. № 5. С. 95–105.

4. Experience of Innovative Technologies Application in the Training for IT Professionals / N. Y. Ershova et al. // Journal on Selected Topics in Nano Electronics and Computing, 2013. Vol. 1, № 1. P. 57–63.

5. Milicchio F.,·Gehrke W. A. Distributed Services with OpenAFS for Enterprise and Education. Berlin : Springer-Verlag, 2007. 395 pp.

6. Мощевикин А. П., Соловьев А. В. Система on-line тестирования iq.karelia.ru // IT-инновации в образовании: Материалы всероссийской научно-практической конференции (27–30 июня 2005 г.). Петрозаводск : Изд-во ПетрГУ, 2005. С. 171–175.

7. Веб-приложение учета успеваемости и посещаемости «Кондуиты» : свидетельство об отраслевой регистрации разработки № 11705 / А.В. Соловьев. № 50200802234 ; заявл. 01.11.2008 ; опубл. 05.12.2008 ; Инновации в науке и образовании, № 46.

8. Никитин С.А., Соловьев А.В. Система учета публикаций // Университеты в образовательном пространстве региона: опыт, традиции, инновации: Материалы научно-методической конф. (16–17 февраля 2010 г.). Петрозаводск, 2010. Ч. II (Л–Я). С. 57–60.

9. Соловьев А.В., Кипрушкин С.А. Вычислительный кластер «Лусидор» как элемент информационно-образовательной среды Физико-технического института ПетрГУ // Ученые записки Института социальных и гуманитарных знаний, 2019. № 1 (17). С. 467–472.

REFERENCES

1. Ershova N.Yu., Nazarov A.I., Soloviev A.V. *Praktika organizatsii uchebnogo protsessa s primeneniem spetsializirovannykh sredstv setevogo obucheniya* [The practice of the educational process arrangement with the use of specialized means of online learning] *Materialy V Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Elektronnaya Kazan'–2013»*, 2013. Issue 1(11), Part II, pp. 58–64.

2. Moschevikin A.P., Soloviev A.V. *Web-servis ucheta poseshchaemosti i uspevaemosti «Konduity»* [«Conduits» the web-service for tracking attendance and progress] *Materialy nauchno-metodicheskoy konferentsii «Universitety v obrazovatel'nom prostranstve regiona: opyt, traditsii i innovatsii» (21–23 noyabrya 2007 g.)*. Petrozavodsk: PetrSU Publ., 2007. Part II, pp. 117–118.

3. Kostjukevich S.H. et al. *Informatsionno-analiticheskaya integrirovannaya sistema PetrGU: podkhody, resheniya, napravleniya razvitiya* [PetrSU Information Analytical Integrated System (IAIS): approaches, solutions, development trends] *Universitetskoe upravlenie: praktika i analiz*, 2015. No. 5, pp. 95–105.

4. Ershova N.Y. et al. Experience of Innovative Technologies Application in the Training for IT Professionals. Journal on Selected Topics in Nano Electronics and Computing, 2013. Vol. 1, No. 1, pp. 57–63.

5. Milicchio F.,·Gehrke W.A. Distributed Services with OpenAFS for Enterprise and Education. Berlin : Springer-Verlag, 2007. 395 p.

6. Moschevikin A.P., Soloviev A.V. *Sistema on-line testirovaniya iq.karelia.ru* [iq.karelia.ru the online test system] *IT-innovatsii v obrazovanii: Materialy vserossiyskoy nauchno-prakticheskoy konferentsii (27–30 iyunya 2005 g.).* Petrozavodsk: PetrSU Publ., 2005, pp. 171–175.

7. Soloviev A.V. Reg. certificate no. 11705. *Veb-prilozhenie ucheta uspevaemosti i poseshchaemosti «Konduity»* [«Conduits» the web-application for tracking attendance and progress], 2008. Innovatsii v nauke i obrazovanii, No. 46.

8. Nikitin S.A., Soloviev A.V. *Sistema ucheta publikatsiy* [Publication tracking system] *Universitety v obrazovatel'nom prostranstve regiona: opyt, traditsii, innovatsii: Materialy nauchno-metodicheskoy konf. (16–17 fevralya 2010 g.).* Petrozavodsk, 2010. Part II, pp. 57–60.

9. Soloviev A. V., Kiprushkin S. A. *Vychislitel'nyy klaster «Lusidor» kak element informatsionno-obrazovatel'noy sredy Fiziko-tekhnicheskogo instituta PetrGU* [«Lucidor» the computing cluster as an element of information and educational environment in Institite of physics and technology of PetrSU] *Uchenye zapiski Instituta sotsial'nykh i gumanitarnykh znaniy*, 2019. No 1 (17), pp. 467–472.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Соловьев Алексей Владимирович

Петрозаводский государственный университет, г. Петрозаводск, Россия, кандидат физико-математических наук, доцент, доцент кафедры информационно-измерительных систем и физической электроники,

E-mail: avsolov@petrsu.ru.

Soloviev Alexei Vladimirovich

Petrozavodsk State University, Petrozavodsk, Russia, Associate Professor of Department of Information Measurement Systems and Physical Electronics, PhD, Assoc. Prof.,

E-mail: avsolov@petrsu.ru.

Корреспондентский почтовый адрес и телефон для контактов с автором статьи:
185910, Респ. Карелия, Петрозаводск, пр. Ленина, 33, ПетрГУ, ФТИ. Соловьев А. В.
+7(8142)71-96-76