ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ И УПРАВЛЕНИЯ УДОСТОВЕРЯЮЩЕЙ ФЕДЕРАЦИЕЙ RUNNetAAI В РАМКАХ ИНТЕРФЕДЕРАТИВНОГО ВЗАИМОДЕЙСТВИЯ С ПРОЕКТОМ eduGAIN

PRINCIPLES OF THE FUNCTIONING AND MANAGEMENT OF THE IDENTITY FEDERATION RUNNetAAI WITHIN THE FRAMEWORK OF INTERFEDERATION WITH eduGAIN

Абрамов Алексей Геннадьевич / Alexey G. Abramov,
к.ф.-м.н., заместитель директора СПб филиала ФГАОУ ДПО ЦРГОП и ИТ / Deputy director of SPb branch of FPAEI CVE CRSEPIT,
abramov@runnet.ru

Васильев Илья Валерьевич / Ilya V. Vasilyev,
ведущий инженер СПб филиала ФГАОУ ДПО ЦРГОП и ИТ / Lead engineer of SPb branch of FPAEI CVE CRSEPIT,
vasilyev@runnet.ru

Порхачёв Василий Александрович / Vasiliy A. Porkhachev,
ведущий специалист СПб филиала ФГАОУ ДПО ЦРГОП и ИТ / Lead specialist of SPb branch of FPAEI CVE CRSEPIT,
porhachev@runnet.ru

Аннотация

В статье приводятся основные термины и определения, организационно-технические принципы построения удостоверяющих федераций, даются общие сведения о международном проекте eduGAIN, в рамках которого осуществляется взаимодействие национальных систем федеративной авторизации, рассматриваются система политик и регламентов, а также базовые механизмы обмена метаданными. Обсуждаются вопросы создания и текущего функционирования удостоверяющей федерации России RUNNetAAI, ее интеграции в проект eduGAIN и подключения к ведущим научным ресурсам.

Abstract

The paper provides the basic terms and the definitions, organizational and technical principles for the building of the identity federations, provides general information about the international project eduGAIN, within the framework of which the interaction with national identity federations is carried out, discusses the system of policies and regulations, as well as the basic mechanisms of metadata exchange. The issues of establish and operating of the identity federation of Russia RUNNetAAI, it's integration with eduGAIN and connection to the leading scientific resources are discussed.

Ключевые слова: национальная научно-образовательная сеть, NREN, RUNNet, федеративная аутентификация, удостоверяющая федерация, AAI, SSO, RUNNetAAI, eduGAIN.

Keywords: national research and education network, NREN, RUNNet, federative authentication, identity federation, AAI, SSO, RUNNetAAI, eduGAIN.

Введение

Проблема обеспечения повсеместного эффективного доступа к научно-образовательным ресурсам и сервисам является сегодня весьма актуальной, особенно в связи с массовым появлением и развитием облачных технологий. Традиционный для университетских кампусов и научных институтов способ организации авторизованного доступа – по фиксиро-

ванным IP-адресам – не удовлетворяет современным требованиям исследователей, преподавателей и студентов [1-3].

Возрастающая мобильность сферы образования и науки обусловила появление новых, более совершенных подходов к организации доступа к таким востребованным ресурсам как информационные базы данных научных публикаций, цифровые коллекции научных данных, а также к веб-сервисам, в том числе в рамках облачных моделей SaaS/PaaS.

Вопросы организации взаимодействия пользователей и поставщиков научно-образовательных ресурсов и сервисов в глобальных сетях на протяжении уже почти двух десятилетий лет успешно решаются в рамках международного проекта eduGAIN, развиваемого панъевропейским научно-образовательным сетевым консорциумом GÉANT [4-5].

Проект eduGAIN (EDUcation Global Authentication INfrastructure, Инфраструктура глобальной аутентификации в интересах образования, http://edugain.org) осуществляет взаимодействие систем федеративной авторизации, эксплуатируемых в разных странах по всему миру, предоставляя возможности доступа к контенту, сервисам и ресурсам глобальному сообществу сферы образования и науки [6, 7].

Федеративная аутентификация понимается здесь как распределенная инфраструктура, которая предоставляет пользователям возможность получать доступ к информационным ресурсам и сервисам научно-образовательных сетей и глобального Интернета по технологии «единого окна» («единого входа» – SSO, Single Sign-On). Наличие такой инфраструктуры существенно упрощает организацию взаимодействия между поставщиком ресурсов и сервисов и конечным пользователем, при этом хранение и обработка персональных данных пользователей производится в полном соответствии с требованиями действующего законодательства [3].

Сегодня eduGAIN объединяет более 60 национальных федераций-участниц по всему миру, в рамках которых функционируют 3 тысячи узлов IdP (провайдеров идентификации, преимущественно, университетов) и более 2300 узлов SP (сервис-провайдеров информационных ресурсов для образования и науки) [7].

К примеру, Великобритания уже делегировала в эту межфедеративную ассоциацию более 500 университетов и колледжей, Франция – почти 300 научных организаций, университетов и т.д. Среди информационных ресурсов, предоставляющих своим пользователям возможность федеративной авторизации, достаточно упомянуть такие организации, как ScienceDirect, Springer, Oxford University Press, IEEE. Сотрудничество с eduGAIN является де-факто обязательным элементом интерфейса современных сетевых электронных ресурсов для науки и образования.

Проекты создания и развития удостоверяющих федераций традиционно реализуются на базе *национальных научно-образовательных сетей* (National Research and Education Network, NREN), под которыми принято понимать информационно-телекоммуникационную сеть, высокопроизводительную телекоммуникационную инфраструктуру масштаба страны, эксплуатируемую исключительно в интересах науки и образования, обеспечивающую доступ целевых пользователей в глобальное ИКТ-пространство, реализующую связность с мировыми NREN и сетевыми консорциумами, а также являющуюся ядром развития и провайдером востребованных сетевых сервисов и сервисов коллективного пользования [8].

В нашей стране функции NREN с 1994 года де-факто выполняет федеральная университетская сеть RUNNet (Russian UNiversity Network, https://www.runnet.ru) [8, 9]. В качестве одного из перспективных направлений работ, выполняемых в настоящее время на базе сети RUNNet, является проект создания и развития *инфраструктуры удостоверяющей федерации национального уровня*, получивший название RUNNetAAI [3, 8-10].

1. Основные термины и определения. Организационно-технические

принципы построения удостоверяющей федерации

В рамках подготовки комплекта необходимых регламентирующих документов специалистами RUNNet был проведен комплекс работ по переводу на русский язык и адаптации к требованиям российских стандартов основополагающих терминов и понятий, определяющих базовые принципы построения и функционирования удостоверяющей федерации [10, 11]. Среди таких терминов и понятий, сформулированных в рамках создания и развития интерфедерации eduGAIN (исходно – на английском языке), можно выделить следующие.

Авторизация – предоставление определенному лицу прав на выполнение определённых действий, а также процесс проверки (и подтверждения) данных прав при попытке выполнения этих действий.

Аутентификация – процедура проверки подлинности пользователя путем сравнения введенных им секретных данных с данными, сохраненными в базе данных пользователей.

Удостоверяющая федерация (УФ) – совокупность участников федерации, присоединившихся к специализированному регламенту (см. рис. 1) в целях информационного сотрудничества посредством безопасного обмена информацией о своих пользователях и ресурсах.

Инфраструктура авторизации и аутентификации – комплекс организационных, технических и юридических решений, предоставляемый оператором УФ ее участникам для авторизации и аутентификации конечных пользователей.

Оператор удостоверяющей федерации – организация, предоставляющая инфраструктуру авторизации и аутентификации для участников УФ.

Домашняя организация – организация, сотрудником или учащимся которой является конечный пользователь; ответственна за аутентификацию конечного пользователя и управление его цифровыми удостоверениями.

Конечный пользователь – физическое лицо, являющееся сотрудником или студентом домашней организации и использующее в своей деятельности ресурсы сервис-провайдеров УФ.

Сервис-провайдер – организация, ответственная за предоставление конечным пользователям доступа к своим защищенным ресурсам.

Интерфедерация – добровольное сотрудничество двух и более удостоверяющих федераций для обеспечения доступа конечных пользователей одной УФ к ресурсам сервис-провайдеров другой УФ.

Одна из ключевых причин, обусловивших широкое распространение принципов и технологий проекта eduGAIN, – продуманная система политик и регламентов, общая схема взаимосвязанности которых приведена на рис. 1.

Регламент (политика) удостоверяющей федерации – основной документ, формулирующий базовые требования к участникам УФ; включает описание управляющих структур федерации, процедур вступления и выхода из состава участников федерации, а также описывает права и обязанности участников и оператора УФ. Остальные документы по своему статусу являются приложениями к регламенту.

Технологический регламент – описывает требования и обязанности оператора и участника УФ в рамках реализации конкретного сервиса. В настоящий момент удостоверяющая федерация RUNNetAAI поддерживает регламент единой точки входа для веб-сервисов (Web Single Sign-On, WebSSO).

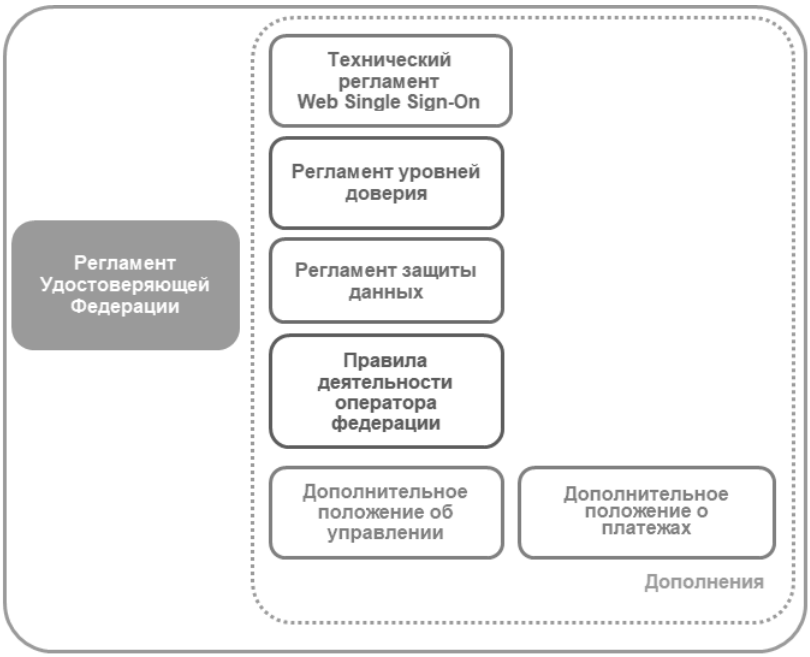

Рис. 1. Система политик и регламентов проекта eduGAIN

Регламент уровней доверия – это документ, который должен быть принят организацией-владелицей узла IdP (иначе говоря, домашней организацией). На основании этого регламента сервис-провайдер может принять решение о степени доверия пользователю и, соответственно, предоставлению ему тех или иных прав на своем ресурсе. Следует отметить, что этот документ находится в разработке сообществом eduGAIN и пока не имеет окончательного вида.

Регламент защиты данных – затрагивает домашние организации и, в первую очередь, – сервис-провайдеров в случаях, когда они обрабатывают персональные данные (этот документ к настоящему моменту также не разработан).

Правила деятельности оператора федерации (ПДО) – описывают процедуры, требуемые к исполнению оператором. Правила позволяют существующим УФ удостовериться в целостности и доступности услуг, систем и конфигурационных данных оператора удостоверяющей федерации (таких, например, как файлы метаданных протокола аутентификации SAML2.0 для WebSSO), а также в том, что оператор обладает подготовленным персоналом. ПДО призваны помочь сторонам понять, какие меры технического характера предпринимает УФ для создания федеративной среды доверия между участниками.

ПДО формируется из пяти практических положений, включающих:

- положение о регистрации метаданных;
- положение о публикации метаданных;
- положение о практике управления ключами;
- положение о практике установления доверия;
- положение о практике мониторинга.

В настоящий момент для участников eduGAIN абсолютно необходимыми являются только первые два документа, которые определяют структуру, формат, обязательные элементы, процедуру регистрации метаданных для узлов участников УФ, а также требования к метаданным федерации в целом.

Представленный набор документов совместно с реализованными технологическими решениями позволяют УФ организовать кросс-доменную среду доверия, в рамках которой каждому новому узлу любой федерации не требуется устанавливать доверительные отношения со всеми остальными узлами в интерфедеративном пространстве, а достаточно лишь следовать разработанным техническим и организационным стандартам.

Важнейшим элементом взаимодействия УФ в рамках интерфедерации eduGAIN является механизм обмена и обработки метаданных [10]. В задачи каждой УФ входит обслуживание конвейера обработки метаданных в формате SAML2.0. Метаданные федерации должны содержать информацию о локальных узлах УФ, отобранных для участия в eduGAIN; формат метаданных при этом должен соответствовать регламенту метаданных интерфедерации. Федерация обязана публиковать метаданные в открытом доступе и предоставить их URL в техническую службу eduGAIN.

Цикл обмена метаданными сводится к следующему (рисунок 2) [12]:

- IdP или SP принимает решение о включении метаданных своего узла в интегральный реестр eduGAIN;
- оператор УФ добавляет метаданные узла в общий исходящий поток ("upstream") метаданных (цифра 1 на схеме);

Metadata Distribution System (система управления реестром метаданных, MDS) eduGAIN:

- собирает и выполняет валидацию входящего ("downstream") потока метаданных от федераций;
- подписывает и вновь публикует метаданные для последующего получения удостоверяющими федерациями (цифра 2 на схеме).

Система управления реестром метаданных УФ:

- принимает метаданные от eduGAIN (цифра 3 на схеме);
- удаляет из полученных метаданных дублирующие записи об узлах, зарегистрированных самой федерацией;
- публикует полученный реестр для использования узлами федерации.

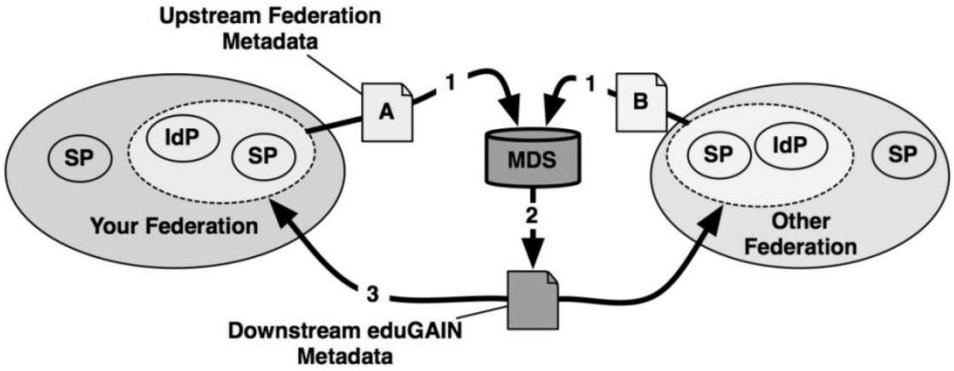

Рис. 2. Цикл обработки метаданных удостоверяющих федераций

В настоящий момент в рамках УФ RUNNetAAI реализован полный цикл взаимодействия с проектом eduGAIN, включая автоматический обмен метаданными.

Весьма полезными при отладке процедур обмена являются онлайн-инструменты eduGAIN по проверке метаданных федерации [10, 12], позволяющие выполнить анализ корректности метаданных и получить следующую информацию:

- сведения о времени регистрации метаданных оператором федерации и выходные данные регистратора;
- сведения о сертификате подписи метаданных, включая метод подписи и длину цифрового ключа;
- сведения о сроке действия метаданных;
- данные по отдельным узлам федерации (наименование узла, URL, контактная информация и пр.).

2. Архитектура и программное обеспечение инфраструктуры удостоверяющих федераций

Для обеспечения цикла сбора (агрегации) метаданных и обмена с eduGAIN

УФ используют сегодня различное программное обеспечение. Наиболее распространенными решениями являются pyFF, реализованное на языке программирования Python, дополнительное ПО для систем управления узлами SimpleSAMLphp (на языке PHP), Shibboleth MA (на языке Java), Jagger (на языке PHP) и собственные разработки федераций.

Наиболее важной концепцией, лежащей в основе систем агрегации метаданных, является концепция конвейера обработки. Конвейер – это компонент, пропускающий коллекцию элементов (в данном случае – метаданных) через несколько этапов обработки, на которых данные могут добавляться, удаляться, трансформироваться и т.п. Как правило, первый этап конвейера состоит в чтении исходных данных из источников данных различного типа (файлы файловой системы, файлы, полученные по HTTP протоколу, конфигурационные файлы и др.), затем производится конструирование данных и, в завершении, заполнение коллекции этими элементами. В случае агрегатора метаданных исходным является XML-документ, который проходит этапы проверки схемы метаданных, проверки цифровой подписи, а потом, в случае необходимости – этап XSLT-трансформации.

В настоящий момент подобную конвейерную обработку реализуют решения Shibboleth MA и pyFF, при этом pyFF является наиболее широко распространенной в мире.

Помимо системы агрегации метаданных УФ используют системы управления федерацией. Чаще всего (но не обязательно) такие системы управления включают в себя функционал агрегатора метаданных. Кроме функции агрегации система управления отвечает за регистрацию узлов федерации, администрирование узлов с включением в тестовую и промышленную среду, сбор статистики и т.д.

RUNNetAAI выбрала для своей работы систему Jagger, разработанную специалистами NREN Ирландии HEAnet. Эта система совмещает функции управления и агрегации метаданных, но процесс агрегации в ней пока недостаточно функционален, в связи с чем, специалистами сети RUNNet были разработаны дополнительные модули обработки. В дальнейшем, при увеличении количества участников RUNNetAAI, и, соответственно, обслуживаемых ими узлов, возможно, потребуется переход на более развитые системы.

3. Текущий статус и основные направления развития проекта RUNNetAAI. Вопросы подключения к ведущим научным ресурсам

В рамках выполненных к настоящему моменту работ по проекту RUNNetAAI следует выделить:

- перевод и адаптацию к российскому законодательству комплекта регламентирующих документов УФ;
- подача заявки на вступление и завершение полного цикла необходимых процедур по оформлению участия RUNNetAAI в проекте eduGAIN в результате чего в апреле 2018 г. RUNNetAAI стала 56-м участником eduGAIN;
- развертывание инфраструктуры федеративной авторизации и аутентификации;
- разработка набора инструкций по развертыванию программного обеспечения узлов для участников федерации;
- развертывание и доработка системы управления УФ RUNNetAAI;
- начало реализации инфраструктуры федеративной авторизации на своих площадках более 10-ю российскими университетами в целях последующего вступления в удостоверяющую федерацию RUNNetAAI.

Настроенные специалистами сети RUNNet сервисы позволили оперативно и результативно провести работы по интеграции процедур авторизации с узлами ряда наиболее востребованных сервис-провайдеров мировой научно-образовательной среды. В целях реализации практических механизмов функционирования УФ RUNNetAAI в качестве таких SP выступили две ведущих мировых базы данных научных публикаций – Web of Science и Scopus (рис. 3).

Web of Science (WoS) – разрабатываемая и предоставляемая компанией Clarivate Analytics поисковая платформа, объединяющая реферативные базы данных публикаций в научных журналах и патентов, в том числе базы, учитывающие взаимное цитирование публикаций. WoS охватывает материалы по естественным, техническим, общественным, гуманитарным наукам и искусству и содержит более 50 миллионов записей.

Scopus – реферативная и аналитическая база научных публикаций и цитирований издательства Elsevier, в которой на текущий момент представлено более 22 тысяч академических журналов от 5 тысяч издательств, включая более 300 российских периодических изданий.

Сегодня данные Scopus и WoS признаны Минобрнауки России в качестве одного из ключевых критериев общероссийской системы оценки эффективности деятельности организаций науки и высшего образования.

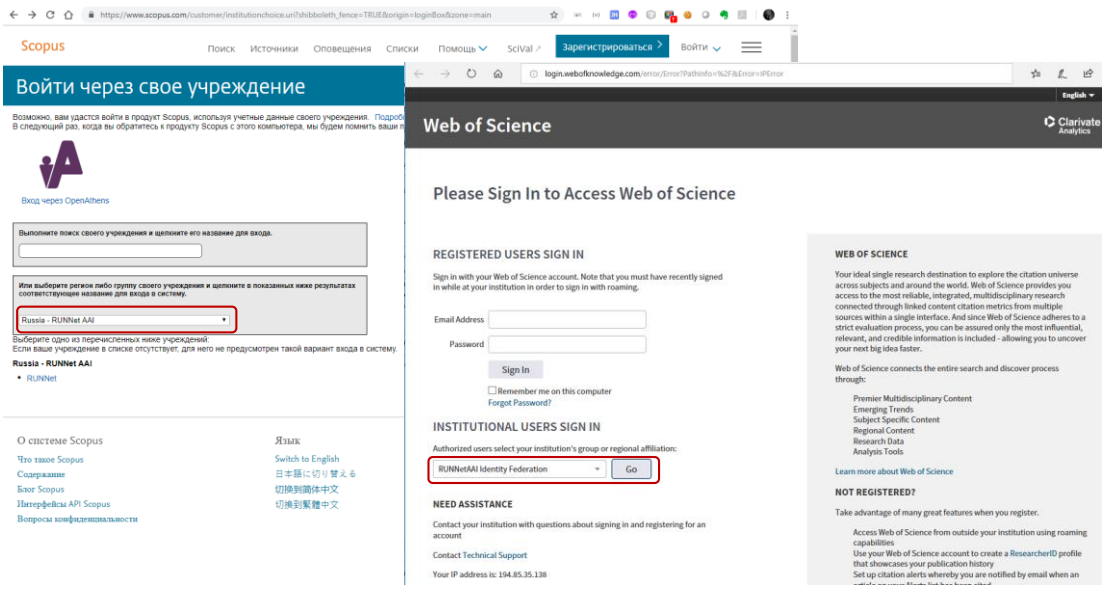

Рис. 3. Федеративная аутентификация на Scopus и WoS через RUNNetAAI

В качестве возможных направлений развития проекта RUNNetAAI специалистами сети RUNNet рассматриваются:

- проведение тематических конференций, семинаров и вебинаров с целью продвижения идей и концепций федеративной аутентификации в профессиональном сообществе страны;
- выработка нормативной документации по использованию технологий федеративной аутентификации в общественных пространствах (вне кампусов университетов и научных организаций);
- поиск и отбор научных ресурсов, представляющих интерес не только для научно-образовательного сообщества России, но и для проекта eduGAIN в целом для последующего включения в УФ RUNNetAAI; расширение пула таких ресурсов не только за счет информационных научных ресурсов, но и путем развертывания сервисов федеративной аутентификации для оборудования центров коллективного пользования сферы образования и науки;
- разработка специализированных модулей программного обеспечения УФ, создание подробных инструкций для пользователей по развертыванию системного программного обеспечения для функционирования узлов федеративной аутентификации и авторизации.

Заключение

В статье приведены ключевые термины и определения, необходимые для корректного описания функционирования удостоверяющих федераций, обозначена система политик и регламентов, формирующая нормативную документацию проекта eduGAIN, рассмотрены основные элементы управления удостоверяющей федерацией, в частности, система управления метаданными с конвейерной обработкой. Представлены текущий статус работ и основные направления развития удостоверяющей федерации России RUNNetAAI.

Статья подготовлена в рамках Государственного задания ФГАОУ ДПО ЦРГОП и ИТ на 2018 год по теме «Разработка и внедрение модели организационно-технологического обеспечения непрерывного функционирования ИКТ-платформы в целях передачи Министерству науки и высшего образования Российской Федерации полномочий и функций управления ресурсами и элементами, реализованными на базе сети RUNNet, по результатам завершения работ».

Литература

1. Chadwick D.W. Federated Identity Management // In: Foundations of security analysis and design V. – Springer Berlin Heidelberg, 2009. – P. 96-120.
2. Bertino E., Takahashi K. Identity Management: Concepts, Technologies, and Systems. – Artech House, 2011. – 198 p.
3. Абрамов А.Г., Васильев И.В., Порхачёв В.А. Развитие инфраструктуры аутентификации и авторизации для удостоверяющей федерации в рамках проектов eduGAIN и eduroam на базе сети RUNNet // ИТНОУ: Информационные технологии в науке, образовании и управлении. – 2017. – №4. – С. 56-64.
4. Официальный сайт проекта GÉANT [Электронный ресурс]. – Режим доступа: http://www.geant.net.
5. Абрамов А.Г. Панъевропейский научно-образовательный сетевой консорциум GÉANT: особенности инфраструктуры, ключевые проекты и сервисы // Информационные технологии. – 2018. – Т. 24. – №8. – С. 546-553.
6. Официальный сайт проекта eduGAIN [Электронный ресурс]. – Режим доступа: https://edugain.org.
7. Hämmerle L., Sabatino R., Lenggenhager T. et al. GN4-1 White Paper: Comparison of Authentication and Authorisation Infrastructures for Research. https://www.geant.org/Resources/Documents/Comparison-of-AAIs-for-Research_White-Paper_v1.0.pdf
8. Абрамов А.Г., Евсеев А.В. RUNNet как национальная научно-образовательная сеть России: цели, основные задачи, телекоммуникационная инфраструктура и сервисы // Информатизация образования и науки. – 2018. – №4(40). – С. 3-15.
9. Абрамов А.Г., Евсеев А.В. Сеть RUNNet: навстречу современным вызовам сферы телекоммуникаций в науке и образовании // Информатизация образования и науки. – 2017. – №1(33). – С. 100-115.
10. Abramov A., Porkhachev V., Vasilyev I. RUNNetAAI Identity Federation of Russia: from deployment to joining eduGAIN // Proc. 3rd CAREN Regional Networking Conference (CRNC2018), Dushanbe, Tajikistan, 23-24 October 2018 [Электронный ресурс]. – Режим доступа: https://crnc2018.icaren.org/files/slides/0003_RUNNetAAI_Identity_Federation_of_Russia_Abramov.pdf.
11. Регламент удостоверяющей федерации RUNNetAAI [Электронный ресурс]. – Режим доступа: https://www.runnet.ru/documents-ru/policy.
12. Wiki eduGAIN [Электронный ресурс]. – Режим доступа: https://wiki.geant.org/display/eduGAIN/.