«Комплексная защита информации»
XVII Международная научно-практическая конференция

Интеграция
в международные электронные инфраструктуры науки – инструмент повышения доверия к национальным научно-образовательным компьютерным сетям

В.В. Анищенко

16 мая 2012 года

ОИПИ

Раздел "Электронные инфраструктуры“ 7-ой РП ЕС

направлен на поддержку инновационного способа проведения научных исследований ("Электронная наука") на основе ИКТ -

путем создания новой среды для фундаментальных и прикладных исследований, в которой виртуальные сообщества:

разделяют,

выделяют и

эксплуатируют совместные мощности европейских научных сервисов:

включая

базы данных,

инструментарий,

вычислительный ресурс и

коммуникации.

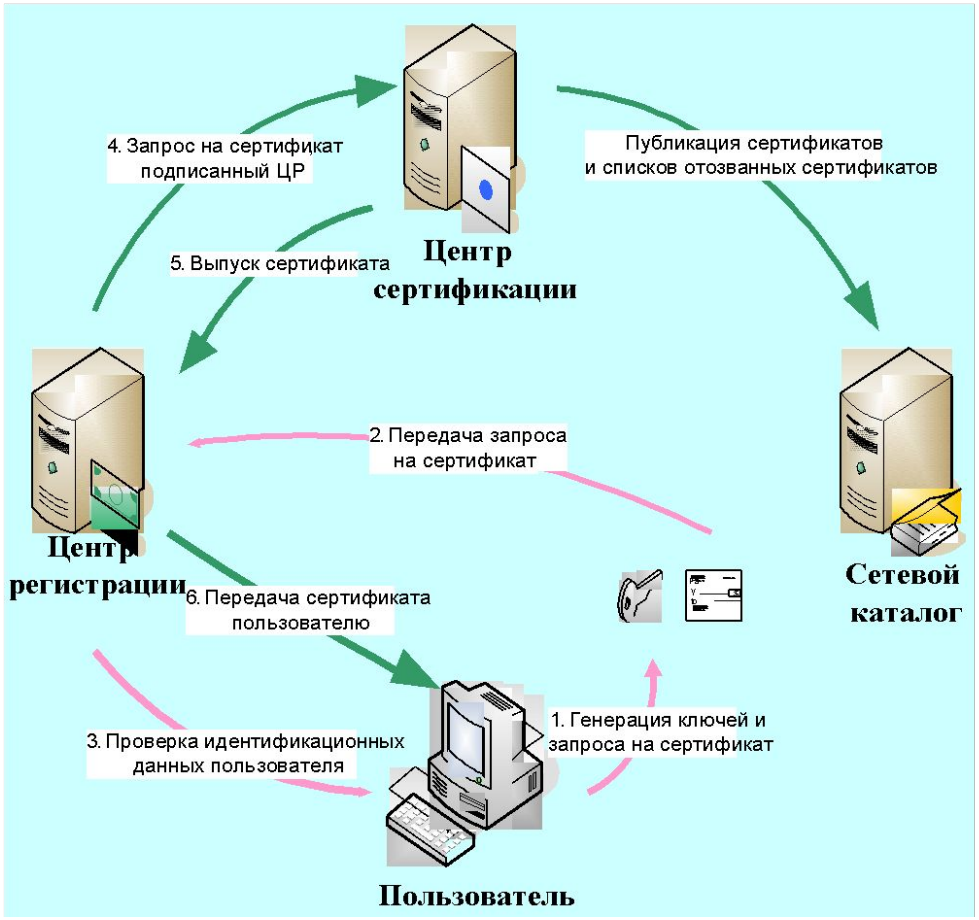
Цели раздела "Электронные инфраструктуры“ 7-ой РП ЕС

- расширить и укрепить высокопроизводительную коммуникационную инфраструктуру научно-образовательной сети GÉANT;
- усилить междисциплинарные Грид и суперкомпьютерные инфраструктуры;
- расширить инфраструктуры научных баз данных;
- поддержать разработку новых вычислительных услуг по обработке данных (петафлопный суперкомпьютинг);
- стимулировать принятие электронных инфраструктур более значительным числом пользовательских сообществ.

Статус НАН Беларуси в международных проектах

- **EGI-InSPIRE (2010 – 2014)** – проект 7 РП ЕС поддержки и развития европейской грид-инфраструктуры, полноправное участие.
- **ORIENTplus (2011 – 2014)** - проект 7 РП ЕС по организации в интересах европейских и китайских научно-образовательных сетей прямого канала связи, полноправное участие.
- **GEANT 3 (2009 – 2013)** - проект 7 РП ЕС по созданию международной инновационной, мультидоменной, гибридной сетевой инфраструктуры GEANT-3 (GN3), ассоциированное участие.

Удостоверяющий центр национальной грид-сети - аккредитованный член EUgridPMA



Общепризнанной метрикой востребованности грид-среды является количество используемых в ней сертификатов. Так с октября 2008 г. удостоверяющим центром ОИПИ НАН Беларуси выдано 235 сертификатов для 108 уникальных физических лиц и 95 серверов из Беларуси. Эти значения являются одним из наиболее важных индикаторов темпов роста и спроса на грид-технологии в стране. Для сравнения, в Литве, Латвии и Эстонии вместе взятых за тот же период было выдано двое меньше сертификатов, однако по оценкам экспертов Еврокомиссии общий (усредненный) результат прибалтийских стран и Беларуси, является очень хорошим даже на фоне таких стран - флагманов грид-технологий как Великобритания, Германия и Италия.

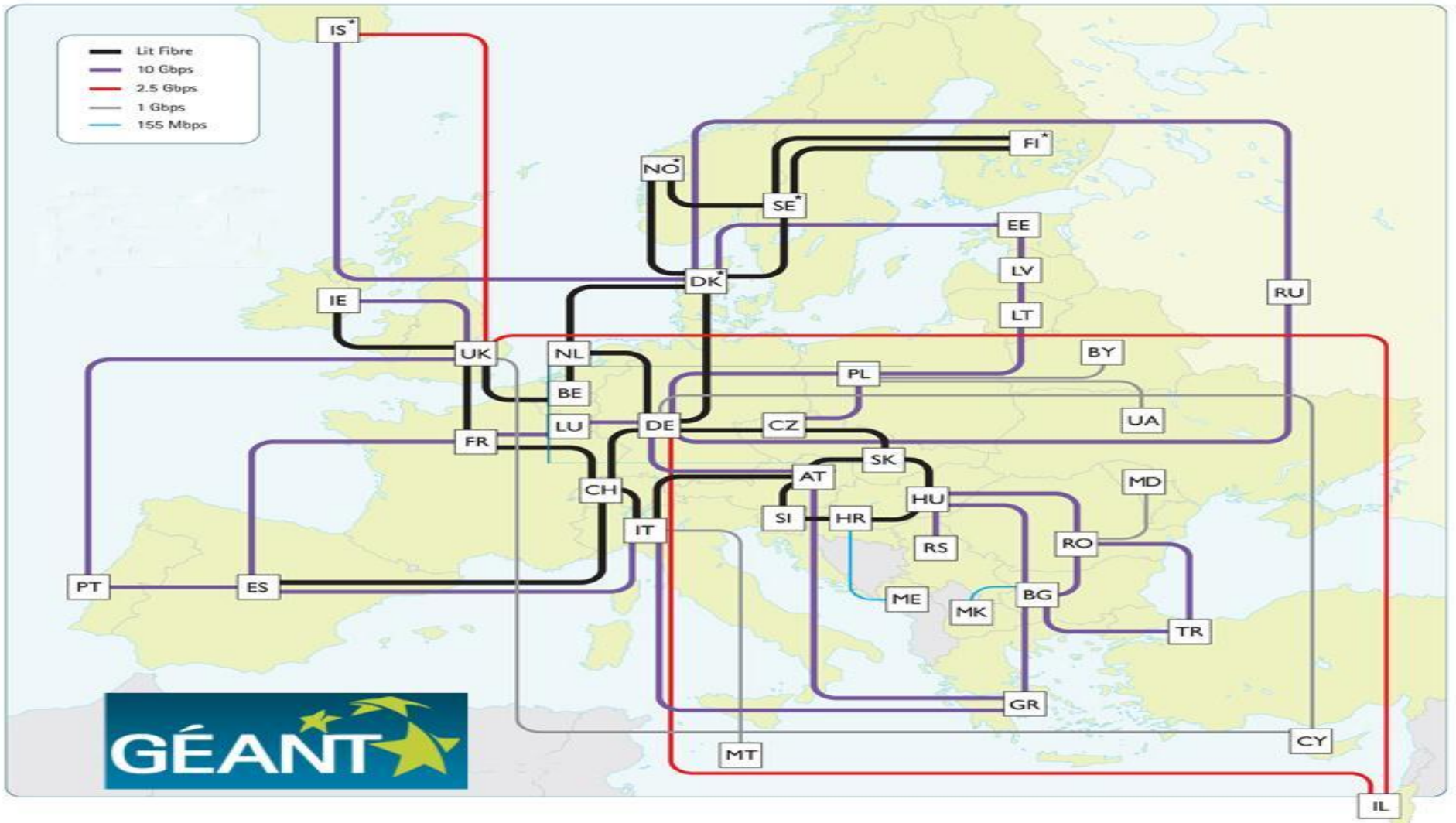
Этапы развития сети GÉANT

- 7-ое поколение европейской научной и образовательной компьютерной сети с федеративной инфраструктурой, которая успешно развивалась на протяжении 20 лет в рамках следующих проектов EC: EuropaNET, TEN34, EN155, GÉANT, GN2 и текущего GN3
- Объединяет 36 стран Европейского Союза через 32 национальные научные сети

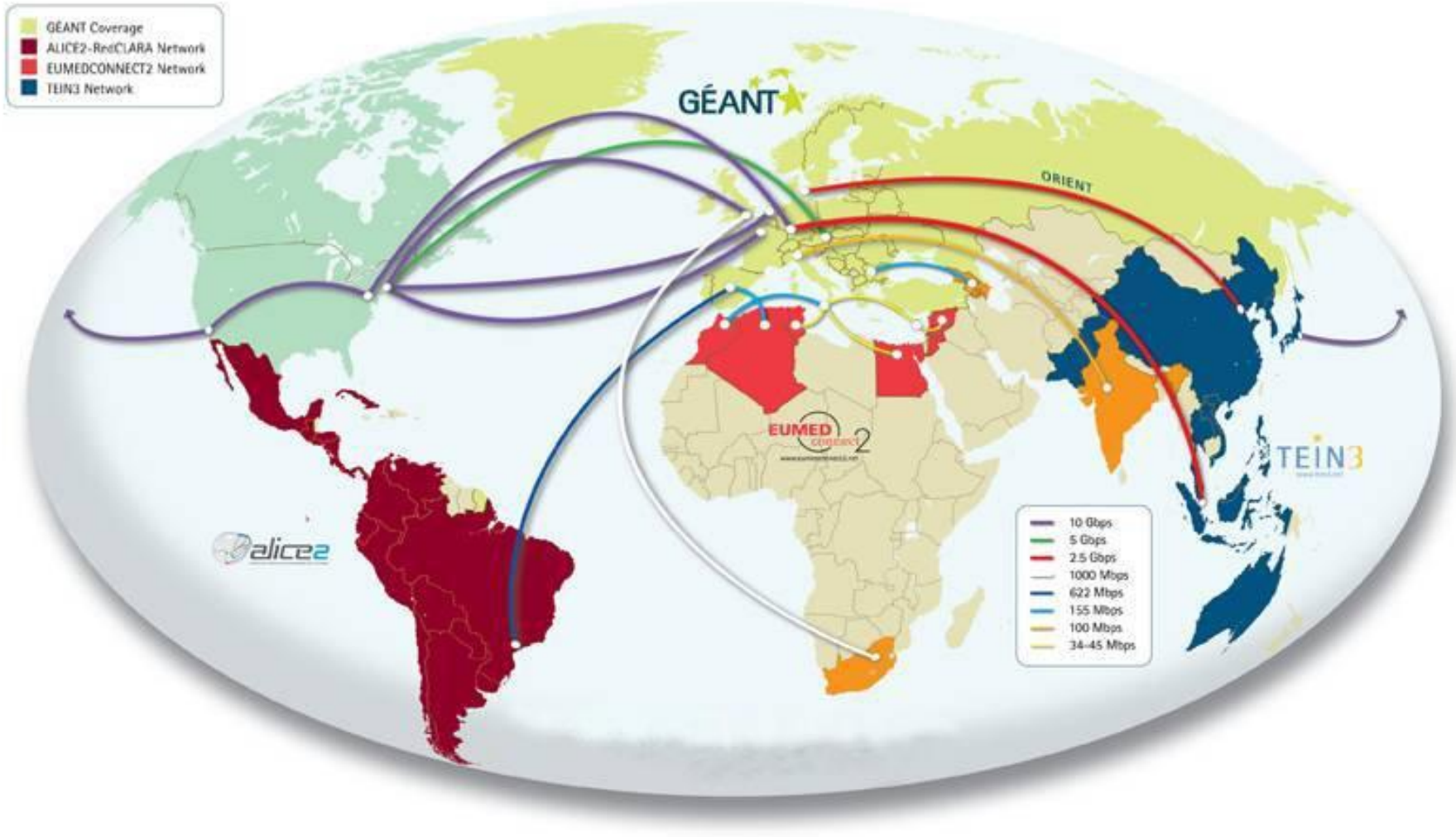
  - обслуживает 4 000 научных и образовательных заведений по всей Европе

  - более 40 000 000 пользователей
- Обеспечивает международные каналы связи в другие регионы планеты
- Управляется Политическим и Исполнительным Комитетами
- Координация и управление от DANTE и TERENA, включая более 400 специалистов разных национальных научных и образовательных сетей.

Топология сети GÉANT



Каналы связи сети GÉANT в другие регионы планеты



Цель проекта GÉANT 3

Проект GÉANT 3 (GN3) создает инновационную, мультидоменную, гибридную сетевую инфраструктуру, которая объединяет конечных научно-исследовательских пользователей и их организации, обеспечивая гибкие и масштабируемые, промышленного качества сервисы в национальных научных и образовательных сетях.

Сервисы сети GÉANT 3

Принципиальной целью проекта GN3 является создание набора мультидоменных сервисов. Эти сервисы формируют базу для развития европейского и глобального научно-исследовательского сотрудничества и разрабатываются Подразделением сервисов (SA) проекта GN3.

Домен - группа ресурсов компьютерной сети под единой политикой управления и администрирования (например, сеть университетского городка или национальная научная и образовательная сеть)

Сервисы сети GÉANT 3

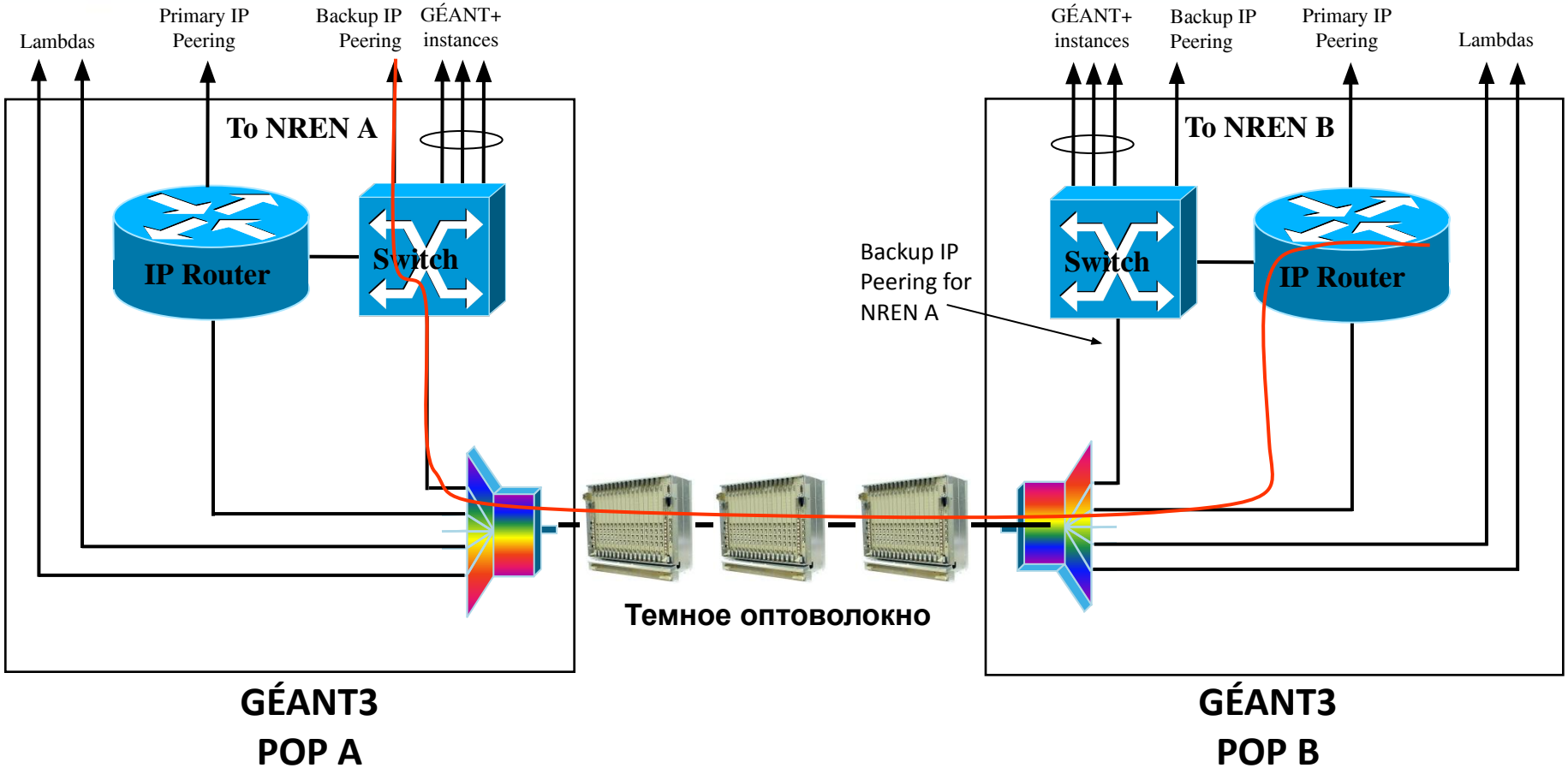
Подразделение сервисов (SA) проекта GN3 включает следующие отделы:
SA1 – Построение и эксплуатация сети Geant
SA2 – Мультидоменные сетевые сервисы
SA3 – Мультидоменные прикладные сервисы для конечных пользователей
SA4 – Управление разработкой программного обеспечения

Сервисы сети GÉANT 3

Сетевые сервисы - сервисы по организации каналов связи для участников проекта (GÉANT IP, GÉANT Plus, GÉANT Lambda, Internet).

- **GEANT IP** сервис предлагает доступ к общей магистральной IP сети Европы. Сервис обеспечивает внутренний IP трафик между Европейскими национальными научными сетями (NRENs) и внешний трафик между Европейскими NRENs и подключенными к GEANT сетями по всему миру.
- **GEANT plus** сервис позволяет NRENs заказывать каналы по технологии точка-точка с пропускной способностью от 155 Мбит/с до 10 Гбит/с в пределах всей текущей сети действующих подключений.
- **GEANT Lambda** сервис предоставляет прозрачные оптические несущие (лямбды) на скорости 10 Гбит/с между точками присутствия сети GEANT (PoPs).

“Гибридная” инфраструктура сети GÉANT



Сервисы GÉANT, обеспечивающие единую безопасную электронную среду науки и образования

Прикладные сервисы – сервисы для конечных пользователей научных и образовательных компьютерных сетей:

eduroam, eduPKI, eduGAIN, educonf, eduPERT, MDM perfSONAR, MDM BoD, MDM Wavelength, GEANT MVPN, Optical private network.

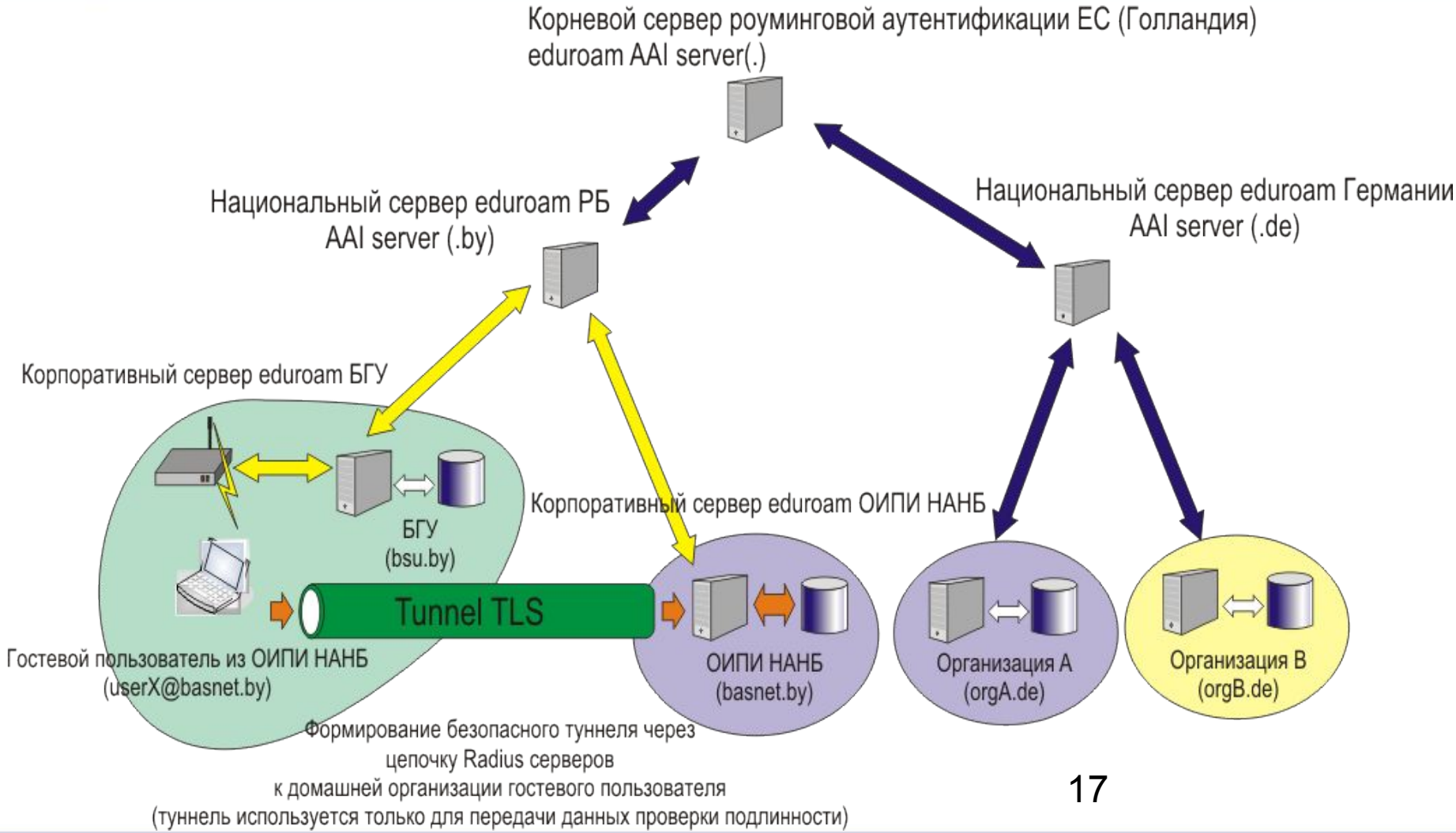
Сервисы GÉANT, обеспечивающие единую безопасную электронную среду науки и образования

- eduroam — сервис роуминговой аутентификации, который позволяет студентам, исследователям и преподавателям, использующим этот сервис, получать свободный сетевой доступ во всех точках, где развернут этот сервис, как внутри страны, так и во время визитов в институты других стран. Свободное WiFi подключение устанавливается сразу после включения портативного устройства;
- eduGAIN — сервис по обеспечению взаимодействия между различными национальными инфраструктурами аутентификации и авторизации (AAI-инфраструктурами);
- eduPERT (PERT - Performance and Enhancement Response Team) — сервис в сети GEANT по диагностированию проблем в компьютерных сетях, выявлению причин перегрузок и отказов сетевых сервисов, техническим аспектам повышения производительности компьютерных сетей, применению современных технологий и инструментальных средств для анализа и исследования сетей;
- perfSONAR — мультидоменный диагностический сервис сетевого мониторинга;
- eduPKI — система доверительного взаимодействия, при которой обслуживаются сервисы в сети GEANT, использующие механизм открытых ключей PKI;

Сервисы GÉANT, обеспечивающие единую безопасную электронную среду науки и образования

- educonf — общеевропейский сервис для организации видеоконференций;
- MDM BoD — мультидоменный сервис запроса пропускной способности, обеспечивающий организацию канала точка-точка определенной пропускной способности, выделенный на какое-то время, для передачи данных между различными доменами для конечных пользователей;
- MDM Wavelength — мультидоменный сервис обеспечения выделенного канала связи с использованием нескольких лямбд из различных доменов;
- GEANT MVPN — сервис виртуальной частной сети на основе сети GEANT;
- Optical private network — сервис оптической частной сети GEANT.

eduroam сервис



eduroam сервис

Пользователь с именем вида userX@basnet.by (гость из ОИПИ) выполняет подключение, например, к сети Белоруского государственного университета (БГУ) в домене bsu.by. При этом корпоративный RADIUS-сервер сети БГУ определяет, что учетная запись подключаемого пользователя userX@basnet.by не принадлежит к домену БГУ, и пересылает запрос на аутентификацию к RADIUS-серверу национального уровня (Federation Level Radius Server - FLRS).

Получив запрос на аутентификацию, национальный RADIUS-сервер обращается за аутентификацией к корпоративному RADIUS-серверу сети ОИПИ и, получив подтверждение действительности учетных данных данного пользователя, пересылает сообщение Access-Accept в сеть БГУ.

Пользователь userX@basnet.by успешно авторизуется в сети БГУ и получает доступ к сетевым ресурсам и в Интернет согласно принятой политики использования данного сервиса.

Аналогично происходит подключение международного студента к сети БГУ, либо студента БГУ при зарубежном визите в любой европейский университет, при этом запрос на аутентификацию дополнительно проходит через корневой сервер роуминговой аутентификации ЕС (Top Level Radius Server - TLRS).

eduPKI сервис

- eduPKI - система доверительного взаимодействия, при которой обслуживаются сервисы в сети GEANT, использующие механизм открытых ключей PKI.
- Цель сервиса eduPKI - упрощение использования и доступа к цифровым сертификатам и инфраструктуре открытых ключей (PKI), определении требований по безопасности сервисов проекта GN3.

eduPKI сервис

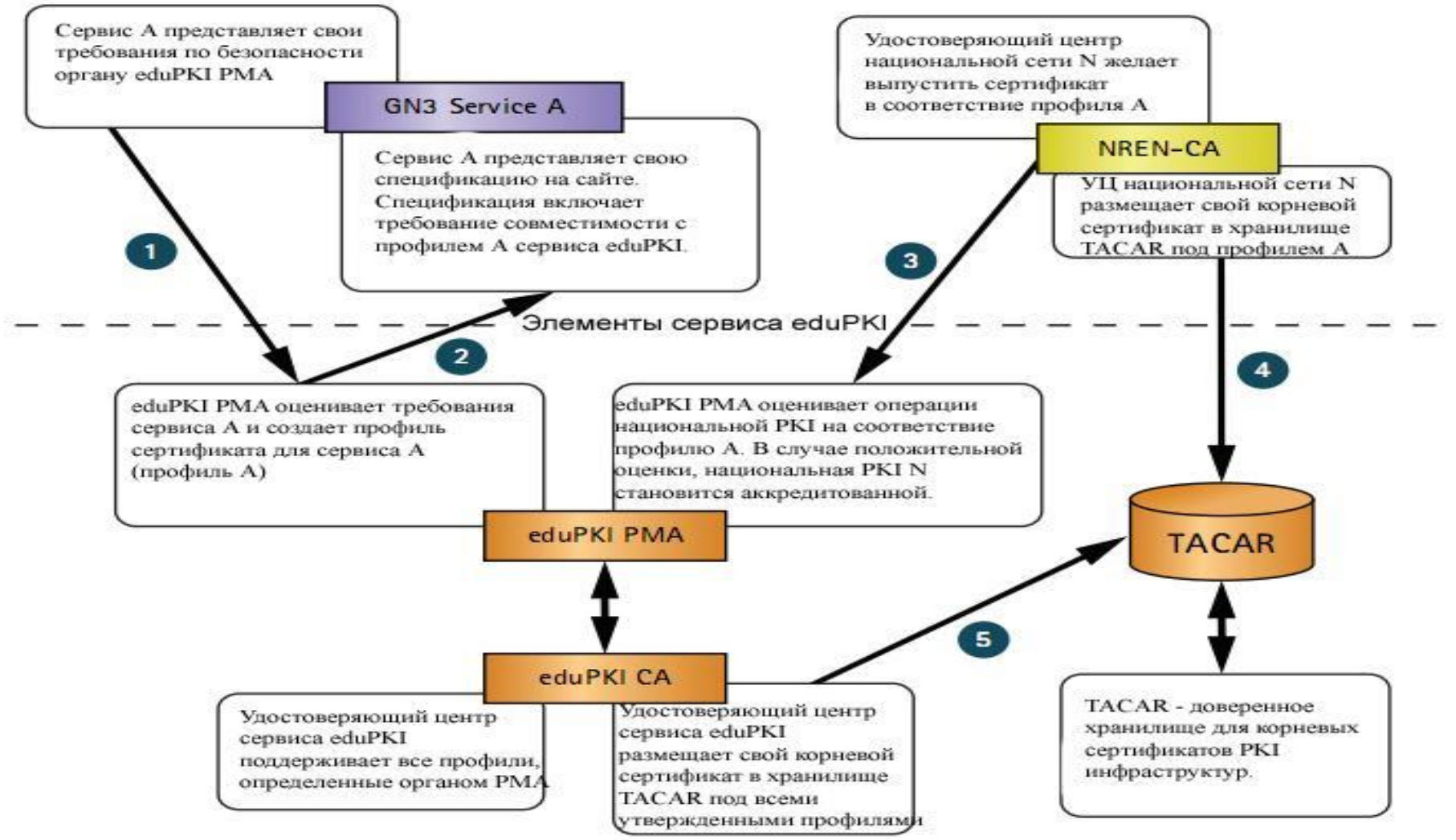


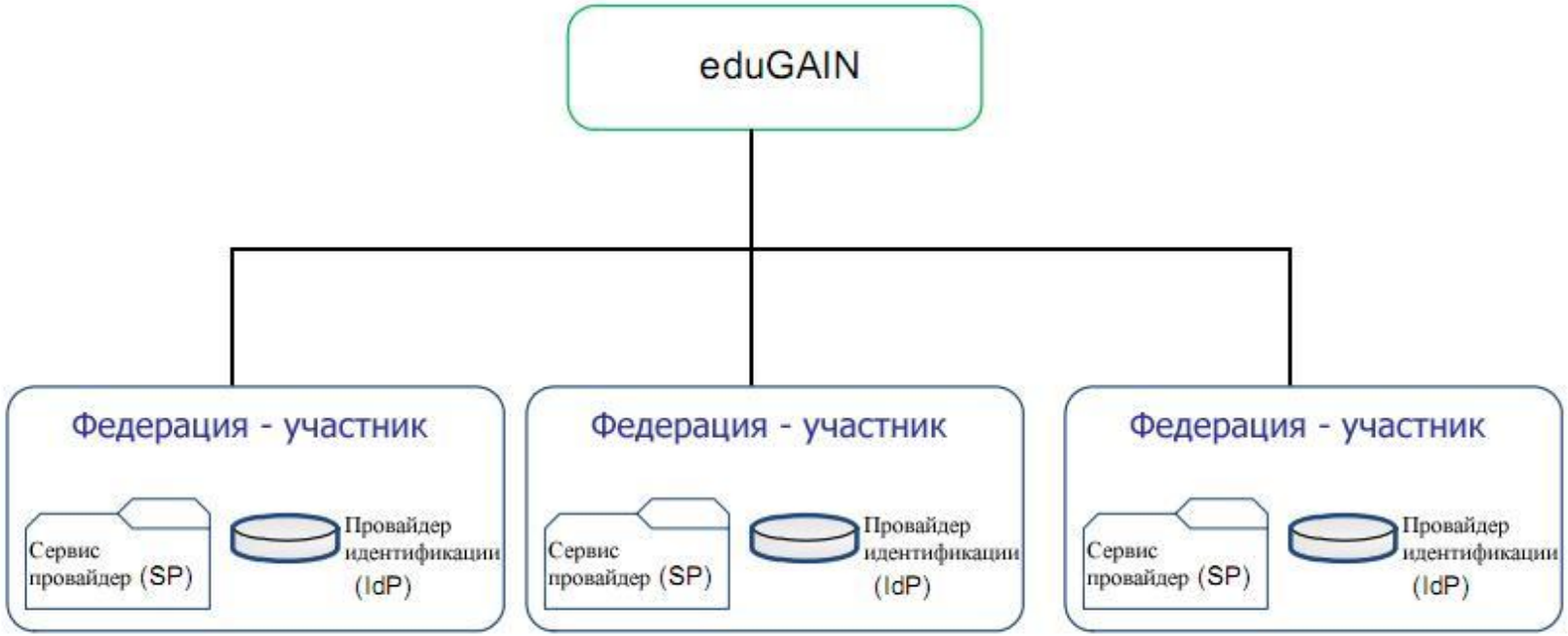
Схема работы eduPKI сервиса

1. Сервис А представляет свои требования по безопасности органу eduPKI PMA.
2. eduPKI PMA оценивает требования сервиса А и создает профиль сертификата для сервиса А (профиль А).
3. Удостоверяющий центр национальной сети N желает выпустить сертификат в соответствие профиля А. eduPKI PMA оценивает операции национальной PKI на соответствие профилю А. В случае положительной оценки, национальная PKI N становится аккредитованной.
4. Удостоверяющий центр национальной сети N размещает свой корневой сертификат в хранилище TACAR под профилем А.
5. Удостоверяющий центр сервиса eduPKI поддерживает все профили, определенные органом PMA. Удостоверяющий центр сервиса eduPKI размещает свой корневой сертификат в хранилище TACAR под всеми утвержденными профилями. Пользователь сервиса А получает сертификат либо в своей национальной PKI, либо в eduPKI.

eduGAIN сервис

- современная технология федеративного доступа к ресурсам научных и образовательных сетей;
- требует развития национальной федерации идентификации для обеспечения доступа к электронной информации в научной и образовательной сфере;
- главное преимущество модели федеративной безопасности состоит в том, что сервисы одной организации могут предоставлять доступ пользователям, которые прошли процедуру аутентификации в домене другой организации.

eduGAIN сервис



Члены национальных федераций получают возможность взаимодействовать друг с другом и использовать единый вход при доступе пользователя ко всем сервисам, предоставляемых федерациями - участниками сервиса eduGAIN. Технология, используемая при обмене идентификационными данными между федерациями, основана на стандарте SAML (Security Assertion Mark-up Language - язык разметки утверждений безопасности).

Перспективы полноправного участия НАН Беларуси в проекте GÉANT3+

- В настоящее время проводятся работы по модернизации прямого волоконно-оптического соединения польской научно-образовательной сети PIONIER с белорусским национальным оператором РУП «Белтелеком». В результате появится возможность дальнейшего расширения пропускной способности канала подключения BASNET к сети Geant до 2.5 - 10 Гбит/с.

- Прорабатывается возможность включения ОИПИ НАНБ в качестве полноправного участника планируемого проекта 7 РП ЕС «GÉANT3+».

- В текущем году завершается реализация 1-й очереди плана создания федеративной инфраструктуры беспроводного широкополосного доступа в Интернет через интеграцию в международную научно-образовательную систему аутентификации eduroam («education roaming») для сотрудников и студентов университетов и научных центров Беларуси.

Благодарю за внимание!

тел. +375 (17) 284 09 85

anishch@newman.bas-net.by