УТВЕРЖДАЮ
Генеральный директор
ОИПИ НАН Беларуси
_____ А.В. Тузиков
"22" 02 2017 г.

Политика национального сегмента Беларуси в общеевропейской системе роуминговой аутентификации eduroam

1. Общие положения

1.1 В документе приводятся основные положения и принципы предоставления сервиса роуминговой аутентификации при доступе в Интернет для научного и образовательного сообщества.

1.2 Eduroam – зарегистрированная торговая марка ассоциации GEANT, являющаяся английской аббревиатурой для словосочетания «роуминг в образовании» («educational roaming»). Сервис по предоставлению удобного, безопасного, масштабируемого доступа в Интернет для гостевых посетителей в любой организации-участнике eduroam разработан в проекте Европейских научных и образовательных компьютерных сетей Geant.

1.3 Подробная информация по eduroam доступна на сайте http://www.eduroam.org

1.4 Документ составлен на основании рекомендаций, приведенных в документе проекта GEANT « Deliverable DJ5.1.3: Roaming policy and legal framework document Part 2: Policy document ».

2. Функции и ответственность участников

2.1 ОИПИ НАН Беларуси как оператор академсети BASNET и национальный представитель Беларуси в европейских научно-образовательных сетях является провайдером национального сегмента сервиса роуминговой аутентификации eduroam в Республике Беларусь.

2.2 ОИПИ НАН Беларуси как провайдер национального сегмента сервиса роуминговой аутентификации eduroam в Республике Беларусь:

2.2.1 отвечает за функционирование национального сегмента сервиса роуминговой аутентификации eduroam и выполняет функции управления политикой национального сервиса eduroam в соответствие с политикой европейской конфедерации сервиса eduroam.

2.2.2 обеспечивает:

– координацию и поддержку сервиса eduroam для определенных контактных лиц от организаций-участников сервиса eduroam,

– поддержание контакта с европейским сообществом сервиса eduroam и обеспечение подключения к серверам аутентификации сервиса eduroam в Европе,

− содействие дальнейшему развитию концепции сервиса eduroam.

2.2.3 отвечает за обеспечение и развитие сетевых подключений национального сервера сервиса eduroam к корпоративным серверам организаций-участников данного сервиса. ОИПИ НАН Беларуси не несет какой-либо ответственности за любые события, возникающие в результате прекращения либо ухудшения функционирования сервиса eduroam.

2.2.4 обеспечивает управление функцией технической поддержки второго уровня при предварительных работах по подключению новой организации-участника сервиса, при эксплуатации сервиса, а также осуществляет поддержку вебсайта национального сервиса eduroam с информацией по правилам функционирования и техническим требованиям сервиса eduroam.

2.2.5 обеспечивает координацию работ и коммуникаций между организациями-участниками сервиса с тем, чтобы политика и правила работы сервиса eduroam соблюдались наилучшим способом, а также имеет право применять технические санкции в случае нарушений.

2.2.6 взаимодействует с контактным лицом от организации-участника сервиса eduroam при проверке работы следующих функций:

− начальное подключение,

− процессы аутентификации и авторизации,

обзор предлагаемого сервиса в организации, включая журналирование требуемых параметров и конфигурацию сервера аутентификации в соответствие с принятой политикой использования сервиса eduroam.

2.3 Провайдер аутентификации

2.3.1 Функцией провайдера аутентификации (домашней организации пользователя) является проверка учетных данных зарегистрированных сотрудников и студентов. Дополнительно провайдер аутентификации осуществляет техническую поддержку для всех своих пользователей, которые хотят воспользоваться сервисом eduroam при поездках в другие организации-участники данного сервиса (гостевые организации пользователя). Только определенные контактные лица организации-участника сервиса eduroam вправе обращаться по вопросам инцидентов и за технической поддержкой для своих пользователей к технической поддержке BASNET.

2.3.2 Провайдеры аутентификации обязаны сотрудничать с ОИПИ НАН Беларуси в случае инцидентов безопасности, нарушения политики и пр. Персонал академсети BASNET будет регистрировать такие случаи при помощи своих инструментов реагирования на инциденты, и принимать соответствующие меры.

2.4 Провайдер ресурсов для сервиса eduroam

2.4.1 Провайдеры ресурсов обязаны сотрудничать с ОИПИ НАН Беларуси в случае инцидентов безопасности, нарушения политики и пр. Персонал академсети BASNET будет регистрировать такие случаи при помощи своих инструментов реагирования на инциденты, и принимать

соответствующие меры.

2.4.2 Функцией провайдера ресурсов для сервиса eduroam является предоставление доступа в Интернет для зарегистрированных пользователей eduroam (для пользователей, прошедших аутентификацию в своей домашней организации посредством инфраструктуры сервиса eduroam). Провайдер ресурсов для сервиса eduroam имеет право авторизовать пользователя для использования других своих сервисов.

2.4.3 О мониторинге активности пользователя необходимо уведомлять пользователей согласно правилам национального законодательства.

2.4.4 Провайдер ресурсов для сервиса eduroam обязуется действовать в рамках национального законодательства, выполнять правила и соблюдать инструкции, перечисленные в данном документе.

2.4.5 Провайдеры ресурсов для сервиса eduroam обязуется сотрудничать с ОИПИ НАН Беларуси.

2.5 Пользователь

2.5.1 Пользователи отвечают за применение своих учетных данных.

2.5.2 Функция пользователя заключается в получении доступа в Интернет через провайдера ресурсов для сервиса eduroam. Пользователь обязан выполнять правила пользования, установленные его провайдером аутентификации (в домашней организации), а также соблюдать правила пользования, установленные в гостевой организации, в которой он получает доступ в Интернет. При обнаружении различий в правилах пользования применяются более строгие правила. Пользователь обязан соблюдать законы страны, в которой он физически находится.

2.5.3 Пользователь отвечает за принятие разумных шагов по проверке того, что он подключается к действительному сервису eduroam (согласно указаниям из домашней организации) до ввода своих учетных данных (логина и пароля).

2.5.4 Пользователи отвечают за свои учетные данные и использование сервиса с их помощью.

2.5.5 При наличии подозрений о раскрытии учетных данных третьей стороне пользователь обязуется сразу сообщить об этом домашней организации.

2.5.6 Пользователь по возможности должен сообщать в гостевую и домашнюю организации обо всех неисправностях сервиса eduroam.

3. Описание системы

3.1 Провайдерам аутентификации необходимо обеспечить эксплуатацию корпоративного сервера аутентификации в соответствие с техническими и административными правилами, приведенными на сайтах http://www.eduroam.by и http://www.eduroam.org; рекомендуется установка второго сервера аутентификации в целях резервирования сервиса.

3.2 Национальный RADIUS сервер сервиса eduroam в сети BASNET должен иметь доступ к корпоративным серверам провайдеров

аутентификации в целях аутентификации и учета.

3.3 Провайдеру аутентификации необходимо создать тестовую учетную запись (учетную запись пользователя сервиса eduroam с логином и паролем), которая будет предоставлена в BASNET для предварительного тестирования, текущего мониторинга, поддержки и поиска неисправностей. При изменении пароля тестовой записи необходимо своевременно отправить уведомление службе поддержки сети BASNET.

3.4 Провайдер ресурсов для сервиса eduroam вправе предоставлять любую среду доступа, однако, минимально необходима поддержка протокола беспроводной связи LAN IEEE 802.11b, рекомендуется применение 802.11g/n.

3.5 Провайдеру ресурсов для сервиса eduroam необходимо обеспечить трансляцию идентификатора беспроводной сети SSID 'eduroam' и поддержку аутентификации по протоколу IEEE 802.1X Extensible Authentication Protocol (EAP) (EAP-TTLS или EAP-PEAP) для создания непрерывного сервиса с соответствующим уровнем безопасности. Трансляцию идентификатора беспроводной сети SSID 'eduroam' необходимо сделать широковещательной.

3.6 Провайдеру ресурсов для сервиса eduroam необходимо обеспечить, по крайней мере, поддержку протоколов IEEE 802.1X и WPA2/AES или лучших.

3.7 Провайдеру ресурсов для сервиса eduroam необходимо обеспечить работу следующих протоколов и портов:

- Standard IPSec VPN: IP протокол, порты ввода-вывода 50 (ESP) и 51 (AH); порт вывода 500/UDP (IKE);
- OpenVPN 2.0: порты ввода-вывода 1194/UDP;
- IPv6 Tunnel broker service: IP протокол, порты ввода-вывода 41
- IPsec NAT-Traversal: порты ввода-вывода 4500/UDP;
- Cisco IPSec VPN over TCP: порт вывода 10000/TCP;
- PTP VPN: IP протокол, порты ввода-вывода 47 (GRE); порт вывода 1723/TCP;
- SSH: порт вывода 22/TCP;
- HTTP: порт вывода 80/TCP, порт вывода 443/TCP, порт вывода 3128/TCP, порт вывода 8080/TCP;
- SMTPS: порт вывода 465/TCP;
- SMTP через STARTTLS: порт вывода 587/TCP;
- IMAP2+4: порт вывода 143/TCP;
- IMAPS: порт вывода 993/TCP;
- POP: порт вывода 110/TCP;
- POP3S: порт вывода 995/TCP;
- Passive (S)FTP: порт вывода 21/TCP.

3.8 Провайдеру ресурсов для сервиса eduroam следует внедрять виртуальную частную сеть (VLAN) для пользователей с eduroam аутентификацией, которую не следует объединять с другими сервисами организации.

3.9 Гостевой институт не должен взимать оплату за eduroam доступ. Этот сервис основан на модели совместного использования подключений к провайдерам ресурсов, когда провайдеры ресурсов сервиса eduroam разных организаций взаимно предоставляют доступ в Интернет для всех пользователей сервиса eduroam.

4. Журналирование

4.1 Провайдеру аутентификации eduroam необходимо сохранять в логах се запросы аутентификации и учета, а именно:

- дату и время поступления запроса на аутентификацию;
- идентификаторы запроса RADIUS – значение атрибута имя пользователя (внешняя идентификация EAP), значение атрибута Calling-Station-Id (MAC-адрес);
- результат аутентификации, возвращаемый провайдером идентификации пользователей;
- причину в случае отказа сервиса или ошибки;
- значение типа в системе учета статуса для данного запроса (тип запроса - начало/конец сессии).

4.2 Провайдеру аутентификации eduroam необходимо сохранять в логах все запросы аутентификации и учета в течение периода минимум 12 месяцев и максимум. Разглашение содержания данных логов должно быть ограничено техническими контактами организации-участника сервиса и техническими контактами BASNET при разрешении случаев нарушения безопасности или политики использования сервиса, о которых сообщено BASNET.

4.3 Провайдеру ресурсов для сервиса eduroam необходимо сохранять в логах все DHCP транзакции, включая:

- дату и время выдачи аренды сетевого адреса через DHCP;
- MAC адрес устройства клиента;
- выданный IP адрес клиента.

4.4 Провайдеру ресурсов для сервиса eduroam необходимо сохранять в логах все DHCP транзакции в течение периода минимум 12 месяцев. Разглашение содержания данных логов должно быть ограничено техническими контактами организации-участника сервиса и техническими контактами BASNET при разрешении случаев нарушения безопасности или политики использования сервиса, о которых сообщено BASNET.

4.5 Провайдеру ресурсов для сервиса eduroam нельзя сохранять в логах какие-либо пароли.

5. Техническое сопровождение

5.1 Провайдер аутентификации осуществляет техническую поддержку для всех своих пользователей, которые хотят воспользоваться сервисом eduroam при поездках в другие организации-участники данного сервиса (гостевая организация пользователя). Только определенное контактное лицо организации-участника сервиса eduroam вправе обращаться по вопросам инцидентов и за технической поддержкой для своих пользователей к технической службе BASNET.

5.2 Провайдеру ресурсов для сервиса eduroam следует оказывать техническую поддержку для пользователей из других организаций, которые хотят воспользоваться сервисом eduroam при своих гостевых визитах в данную организацию.

5.3 Провайдеру ресурсов для сервиса eduroam необходимо опубликовать информацию о локальных особенностях сервиса eduroam на определенных страницах вебсайта данной организации, при этом необходимо указать по крайней мере следующую информацию:

- декларацию о согласии с правилами (с указанием ссылки в Интернет) данной национальной политики сервиса eduroam, опубликованной на вебсайте http:// www .eduroam.by;
- ссылку в Интернет на правила пользования сетевыми ресурсами провайдера ресурсов для сервиса eduroam;
- список либо карту с указанием областей покрытия сервиса eduroam;
- подробности с указанием о широковещательном идентификаторе беспроводной сети SSID eduroam;
- подробности процесса аутентификации и предлагаемых сервисах при авторизации;
- подробности о непрозрачных прокси приложениях при наличие таковых с инструкцией по настройке;
- ссылку в Интернет на вебсайт http://www.eduroam.by с размещением логотипа сервиса eduroam и указанием правообладателя этой торговой марки;
- в случае мониторинга сетевой активности клиента, провайдеру ресурсов для сервиса eduroam необходимо явно указать об этом со ссылкой на национальное законодательство и информацией о времени хранения данных мониторинга;
- контакты ответственного лица по технической поддержки сервиса eduroam организации-участника сервиса.

6. Связи с общественностью

6.1 Провайдеру аутентификации eduroam необходимо предоставить ОИПИ НАН Беларуси контактные данные, по крайней мере, двух человек технической поддержки организации-участника сервиса. О любых изменениях этой информации необходимо своевременно уведомлять ОИПИ НАН Беларуси.

6.2 Провайдеру ресурсов для сервиса eduroam необходимо выделить персонал для работы с инцидентами безопасности при эксплуатации сервиса. Данное контактное лицо может совпадать с номинированным сотрудником технической поддержки сервиса eduroam.

6.3 Организациям-участникам необходимо своевременно уведомлять персонал BASNET о следующих инцидентах:

- инциденты нарушения безопасности;
- неправильное использование;
- отказы сервиса;
- изменения в статусе пользователей или домена при инцидентах.

7. Ответственность, контроль над соблюдением политики, санкции

7.1 ОИПИ НАН Беларуси как оператор академсети BASNET является руководящим органом по реализации и соблюдению данной политики.

7.2 Любые изменения данной политики должны выполняться с участием организаций-участников и ОИПИ НАН Беларуси.

7.3 Подключение к национальному серверу корпоративного сервера организации-участника сервиса eduroam подразумевает принятие организацией данной политики.

7.4 В случаях, когда требуется немедленное вмешательство для обеспечения целостности и безопасности сервиса eduroam, персонал BASNET имеет право отключить сервис либо ограничить его использование для тех организаций-участников, к которым относятся необходимые изменения. При этом персонал BASNET отправляет уведомления организациям-участникам об инцидентах, неисправностях и мерах по восстановлению.

7.5 Персонал BASNET отправляет уведомления по электронной почте контактным лицам, ответственным за сервис eduroam в организации-участнике, о технических нарушениях, несоблюдению политики либо об инцидентах безопасности, по которым требуется принять меры. В случае отсутствия своевременного реагирования либо в случае угрозы целостности и безопасности сервиса eduroam, персонал BASNET имеет право отключить доступ к сервису данной организации-участнике.

7.6 Провайдер ресурсов для сервиса eduroam может запретить использование сервиса для всех пользователей определенной организации-участника путем конфигурирования своего корпоративного сервера аутентификации на блокировку определенной доменной зоны, в некоторых случаях допускается блокировка провайдером ресурсов для сервиса eduroam выделенного гостевого пользователя.

7.7 Провайдер аутентификации eduroam может ограничить доступ определенного пользователя к сервису eduroam путем внесения изменений в конфигурацию сервера аутентификации или удалением данного пользователя из базы данных учетной информации пользователей.

7.8 Провайдеру аутентификации eduroam необходимо также предусмотреть процедуру воздействия на пользователя, нарушающего правила пользования, независимо от его географического местонахождения в момент нарушения.

8. Словарь сокращений

AH:	Authentication Header	заголовок аутентификации
AUP:	Acceptable Usage Policy	правила пользования
CERT:	Computer Emergency Response Team	Группа Реагирования на Инциденты Компьютерной безопасности
DHCP:	Dynamic Host Configuration Protocol	протокол динамического конфигурирования хост-машин
EAP:	Extensible Authentication Protocol	расширяемый протокол аутентификации
eduroam:	educational roaming	роуминговая аутентификация в образовании
ESP:	Encapsulating Security Payload	полезная нагрузка со встроенной защитой
FTP:	File Transfer Protocol	протокол передачи файлов
GRE:	Generic Routing Encapsulation	общая инкапсуляция маршрутов
HTTP:	Hypertext Transfer Protocol	гипертекстовый транспортный протокол
HTTPS:	Secured HTTP	защищенный гипертекстовый транспортный протокол
IEEE:	Institute of Electrical and Electronics Engineers	институт инженеров электротехники и электроники
IKE:	Internet Key Exchange	протокол обмена ключами в Интернете
IMAP:	Internet Message Access Protocol	протокол доступа к сообщениям Интернет
IMAPS:	Secured IMAP	защищенный протокол доступа к сообщениям Интернет
IP:	Internet Protocol	протокол межсетевого обмена IP
IPSec:	IP Secured	защищенный протокол межсетевого обмена
LAN:	Local Area Network	локальная компьютерная сеть
MAC:	Media Access Control	управление доступом к среде передачи данных
MD5:	Message Digest algorithm (version 5)	алгоритм представления сообщения в краткой форме (версия 5)
NAT:	Network Address Translation	трансляция сетевых адресов

POP3:	Post Office Protocol	протокол электронной почты
PPTP:	Point to Point Tunneling Protocol	протокол туннелирования точка-точка
RADIUS:	Remote Authentication Dial In User Service	служба удалённой аутентификации пользователей
RDP:	Remote Desktop Protocol	протокол удаленного рабочего стола
RFC:	Request For Comments	документ RFC
SMTP:	Simple Mail Transfer Protocol	протокол электронной почты Интернет
SMTPS:	Secured SMTP	защищенный протокол электронной почты Интернет
SSH:	Secured Shell	защищенная командная оболочка
SSID:	Service Set Identifier	идентификатор беспроводной сети
TCP:	Transmission Control Protocol	протокол управления передачей
TERENA:	Trans European Research and Education Networking Association	Общеевропейская ассоциация научных и образовательных сетей
TKIP:	Temporal Key Integrity Protocol	протокол шифрования с использованием временных ключей
TLS:	Transport Layer Security	безопасность на транспортном уровне
TTLS:	Tunneled TLS	защищенная безопасность на транспортном уровне
UDP:	User Datagram Protocol	протокол пользовательских дейтаграмм
VLAN:	Virtual LAN	виртуальная локальная компьютерная сеть
VPN:	Virtual Private Network	виртуальная частная сеть
WEP:	Wired Equivalent Privacy	протокол защиты данных WEP
Wifi:	Wireless Fidelity	беспроводной интернет WiFi
WPA:	Wifi Protected Access	протокол защиты данных WPA