Регламент Российской Удостоверяющей Федерации Eduroam

1 Общие сведения

1. Цель Российской Удостоверяющей Федерации Eduroam - обеспечить легкий защищенный и контролируемый доступ к сетям науки и образования мобильных пользователей организаций, участвующих в Федерации.
2. Настоящий документ содержит правила предоставления роуминга в научно-образовательных сетях. Правила разработаны и утверждены Национальной ассоциацией исследовательских и научно-образовательных электронных инфраструктур e-Arena. Правила обязательны для всех участников Российской Удостоверяющей Федерации Eduroam.
3. Оператором Федерации является Межведомственный суперкомпьютерный центр Российской академии наук — филиал Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» (МСЦ РАН – филиал ФГУ ФНЦ НИИСИ РАН).
4. Регистратором Федерации является:
   - Межведомственный суперкомпьютерный центр Российской академии наук — филиал Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» (МСЦ РАН – филиал ФГУ ФНЦ НИИСИ РАН).
   - Федеральное государственное автономное образовательное учреждение дополнительного профессионального образования "Центр реализации государственной образовательной политики и информационных технологий» (ФГАОУ ДПО ЦРГОП и ИТ)
5. Участниками Российской Удостоверяющей Федерации Eduroam могут быть любые организации науки и образования Российской Федерации.
6. Eduroam – зарегистрированный товарный знак организации TERENA, который является сокращением от “educational roaming”, берет свое начало от проекта европейских национальных научно-образовательных сетей по созданию удобного, безопасного и масштабируемого решения по предоставлению доступа в Интернет для посетителей научных и образовательных организаций.
7. Полная информация о Европейской Конфедерации Eduroam представлена на сайте http://www.eduroam.org.

2 Роли и ответственность

2.1 Оператор

1. Оператор отвечает за:
   - разработку, развитие и поддержку национальной сети серверов авторизации, к которым подключаются организации и участники eduroam, баз данных и сервисов eduroam на национальном уровне;
   - обеспечивает взаимодействие национальной и европейской инфраструктур eduroam;

- обеспечивает техническую поддержку Регистраторам Российской Удостоверяющей Федерации Eduroam.

2. Оператор не несет ответственности за последствия и потери, вызванные прерыванием или нарушением сервисов. Провайдеры аутентификации и сервис-провайдеры (независимо от того находятся они в одной Удостоверяющей Федерации или разных) не несут друг перед другом ответственности за последствия и потери, вызванные прерыванием или нарушением сервисов.
3. Оператор отвечает за техническую поддержку и обслуживание национального сайта (http://eduroam.ru), который содержит административные и технические регламенты, техническую документацию сервисов eduroam.
4. Оператор отвечает за взаимодействие с Регистраторами для своевременного выполнения правил и процедур, описанных в настоящем регламенте и в самом крайнем случае имеет право налагать технические санкции.

2.2 Регистратор

1. Регистратор Российской Удостоверяющей Федерации Eduroam (Регистратор) - организация уполномоченная обеспечивать технические мероприятия и поддержку по подключению организаций науки и образования к eduroam и управления группами доступа в национальной инфраструктуре eduroam.
2. Регистратор:
   - обеспечивает поддержку сервера(ов) групп национальной инфраструктуры eduroam;
   - вносит информацию о подключаемых организациях в базы данных российской инфраструктуры eduroam;
   - обеспечивает технические мероприятия по подключению организации к российской инфраструктуре eduroam;
   - обеспечивает техническую поддержку организациям, подключенных им к eduroam.
3. Регистратор работает только с уполномоченными организацией-участником eduroam ответственными лицам по техническим вопросам.
4. Регистратор предоставляет техническую поддержку подключенным организациям по следующим вопросам:
   - начальное подключение;
   - процессы аутентификации и авторизации;
   - предлагаемые сервисы авторизации, проверка логов и конфигурации сервера аутентификации на соответствие требованиям правил и регламентов Российской Удостоверяющей Федерации Eduroam.
5. Регистраторы отвечают за взаимодействие между организациями-участниками eduroam для своевременного выполнения правил и процедур, описанных в настоящем регламенте и, в самом крайнем случае, имеют право налагать технические санкции.
6. Регистратор обязан своевременно информировать Оператора об инцидентах безопасности, злоупотреблениях и отказах сервиса, о которых его информируют организации-участники.

2.3 Провайдер идентификации (IdP)

1. Провайдер идентификации (домашняя организация, Identity Provider, IdP) - организация-участник eduroam, которая предоставляет своим сотрудникам и студентам учетные записи для использования eduroam и обеспечивает их аутентификацию в инфраструктуре eduroam.
2. Провайдер идентификации обязан соблюдать настоящие правила и следовать процедурам, определенным в настоящем Регламенте.
3. Провайдер идентификации обязан обеспечивать техническую поддержку своим пользователям, использующим eduroam при посещении других организаций.
4. Провайдер идентификации обязан извещать Регистраторов об инцидентах безопасности, о которых его информируют пользователи. Только уполномоченные представители Провайдера идентификации могут обращаться к Регистраторам за технической поддержкой или извещать об инцидентах безопасности от имени своих пользователей.
5. Провайдер идентификации должен предупредить своих пользователей об условиях роуминга, особенно обязанностей пользователей. Провайдер идентификации обязан информировать своих пользователей об основах и рекомендациях по обеспечению безопасности.
6. Провайдер идентификации должен сотрудничать с Регистраторами и Оператором во всех вопросах, связанных с eduroam. При расследовании инцидентов безопасности с участием его пользователей Провайдер идентификации не обязан предоставлять протоколы или иные данные, кроме требуемых в соответствии с законодательством.

2.4 Сервис-провайдер (SP)

1. Сервис-провайдер обеспечивает доступ к Интернет и ресурсам своей сети с использованием аутентификации пользователей через eduroam (опираясь на ответ домашней организации (Провайдера идентификации) о результатах аутентификации). Сервис-провайдер авторизует использование любых предоставляемых им сервисов.
2. Сервис-провайдер обязан соблюдать настоящие правила и следовать процедурам, определенным в настоящем Регламенте.
3. В случаях мониторинга активности пользователей Сервис-провайдер обязан явно объявить об этом, включая то, как осуществляется мониторинг, хранение и доступ к собираемым данным в соответствии с законодательством.
4. Сервис-провайдер обязан сотрудничать с Регистраторами и Оператором во всех вопросах, связанных с eduroam.
5. Только уполномоченные представители Сервис-провайдера могут обращаться к Регистраторам за технической поддержкой или извещать об инцидентах безопасности.

2.5 Пользователи

1. Пользователь - лицо, которое получает доступ к Интернет и сетевым ресурсам Сервис-провайдера. Пользователь обязан соблюдать правила использования сети

домашней организации (Провайдера идентификации) и посещаемой организации (Сервис-провайдера). Если правила различаются, пользователь должен подчиняться более строгим правилам.

2. Пользователь отвечает за сохранение своих учетных данных (логин и пароль), их использование, за использование сервисов, предоставляемым по этим учетным данным.
3. Пользователь должен принять разумные меры для проверки того, что он подключается к подлинному сервису eduroam (в соответствии с указаниями их домашней организации) до ввода своих учетных данных. Это означает использование взаимной проверки подлинности (проверки сертификата RADIUS-серверов перед вводом своих учетных данных) и подключение только к защищенной сети 802.1X.
4. Если пользователь имеет основания предполагать, что его пароль стал известен посторонним (скомпрометирован), он должен немедленно сообщить об этом в свою домашнюю организацию (своему Провайдеру идентификации).
5. Пользователь обязан информировать организацию, которую посещает (по возможности) и домашнюю организацию обо всех перебоях сервиса eduroam или подозрениях о нарушениях безопасности.

3 Базовые сервисы

1. Провайдер идентификации должен развернуть сервер аутентификации в соответствии с техническими и административными требованиями, описанными на сайте http://www.eduroam.ru. Рекомендуется использовать резервный сервер аутентификации для повышения надежности. Сетевое оборудование и программное обеспечение должно соответствовать RFC 2865 (RADIUS).
2. Сервер аутентификации должен отвечать на запросы национальных серверов по аутентификации и учету.
3. Провайдер идентификации обязан создать тестовую учетную запись (имя пользователя и пароль), который будет использоваться Регистратором для предварительного тестирования при подключении, постоянного мониторинга, поддержки и поиска неисправностей. Если пароль тестовой учетной записи был изменен, необходимо своевременно уведомить об этом Регистратора. Тестовая учетная запись не должна предоставлять доступа ни к каким сервисам, требующим авторизации.
4. Сервис-провайдер может предоставлять доступ с использованием любых технологий, как минимум сервис-провайдер обязан предоставить беспроводную сеть по стандарту IEEE 802.11g (рекомендуется 802.11a/g/n).
5. Сервис-провайдер обязан использовать SSID "eduroam" (маленькими буквами). SSID eduroam должен быть широковещательным. В случаях, когда зоны сервиса eduroam, предоставляемого двумя разными организациями, пересекаются и для пользователя является критичным подключение к конкретной организации, допустимо использование SSID вида "eduroam-организация".
6. Сервис-провайдер должен использовать аутентификацию по протоколу IEEE 802.1X Extensible Authentication Protocol (EAP) с интерфейсом RADIUS для подключения к инфраструктуре eduroam. Беспроводные сети IEEE 802.11i должны

поддерживать WPA2+AES и могут поддерживать WPA+TKIP для совместимости с устаревшим оборудованием.

7. Сервис-провайдер должен обеспечить передачу трафика к пользователям eduroam и от них в соответствии со следующими минимальными требованиями:
   - Стандартный IPSec VPN:
     - IP протокол 50 (ESP) входящий и исходящий
     - IP протокол 51 (AH) входящий и исходящий
     - UDP/500 (IKE) исходящий
   - OpenVPN 2.0: UDP port 1194 входящий и исходящий
   - IPv6 Tunnel broker service: IP протокол 41 входящий и исходящий
   - IPSec NAT-Traversal: UDP/4500 входящий и исходящий
   - Cisco IPSec VPN over TCP: TCP/10000 исходящий
   - PPTP VPN:
     - IP протокол 47 (GRE) входящий и исходящий
     - TCP/1723 исходящий
   - SSH: TCP/22 исходящий
   - HTTP:
     - TCP/80 исходящий
     - TCP/443 исходящий
     - TCP/3128 исходящий
     - TCP/8080 исходящий
   - Отправка почты:
     - TCP/465 исходящий
     - TCP/587 исходящий
   - Прием почты:
     - TCP/143 исходящий
     - TCP/993 исходящий
     - TCP/110 исходящий
     - TCP/995 исходящий
   - FTP (passive): TCP/21 исходящий
   - RDP: TCP/3389 исходящий
8. Сервис-провайдер должен предоставить для пользователей, аутентифицированных с использованием eduroam, выделенную виртуальную локальную сеть (VLAN).
9. Сервис-провайдер вправе предоставить разным группам пользователей разные привилегии доступа к своим ресурсам (используя механизм групп). При этом разные группы пользователей могут попадать в разные виртуальные локальные сети (VLAN).
10. Сервис-провайдер не должен взимать плату за доступ в свою сеть и Интернет с использованием eduroam. Сервис eduroam основан на использовании разделяемой модели доступа, при которой сервис-провайдеры предоставляют и получают доступ в Интернет для их пользователей.

4 Протоколирование

1. RADIUS-сервер Провайдера идентификации должны протоколировать следующее события:

- дату и время получения запроса на аутентификацию;
- идентификатор запроса RADIUS;
- имя пользователя;
- результат аутентификации, который получен от сервера вышестоящего уровня или локального сервиса (базы данных) аутентификации

2. RADIUS-сервер Сервер-провайдера и Провайдера идентификации должны протоколировать следующее события:
   - дату и время получения запроса на аутентификацию;
   - идентификатор запроса RADIUS;
   - MAC-адрес клиента;
   - имя пользователя и его домен (realm);
   - результат аутентификации, который получен от сервера вышестоящего уровня или локального сервиса (базы данных) аутентификации
3. Сервис-провайдер должен протоколировать все транзакции DHCP, включая:
   - дату и время выделения адреса;
   - MAC-адрес клиента;
   - выделенный IP-адрес.
4. Срок хранения протоколов определяется Российским законодательством и рекомендациями Российской Удостоверяющей Федерации Eduroam. К протоколам допускается только уполномоченный технический персонал провайдера, Регистраторов и Оператора для расследования случаев нарушения безопасности или злоупотреблений, о которых были проинформированы Регистратор и/или Оператор.

5 Поддержка пользователей

1. Провайдер идентификации должен обеспечивать техническую поддержку своим пользователям при их подключении к eduroam у Сервис-провайдера.
2. Сервис-провайдер должен оказывать поддержку пользователям других организаций при их подключении к eduroam у Сервис-провайдера.
3. Сервис-провайдер должен опубликовать на выделенной странице сайта организации информацию о сервисе eduroam в следующем минимально необходимом объеме:
   - текст, подверждающий соблюдение настоящего Регламента и ссылку на него;
   - ссылку на правила использования сети Сервис-Провайдера;
   - карту покрытия или описание области покрытия eduroam;
   - используемый для eduroam SSID;
   - используемый процесс идентификации и список сервисов, для которых нужна авторизация;
   - список непрозрачных прокси-серверов и описание необходимых настроек пользователей (если используются);
   - ссылку на сайт eduroam.ru и логотип eduroam;
   - в случае мониторинга сетевой активности пользователей (кроме описанного в настоящем регламенте протоколирования) объявление о нем, включая то, как осуществляется мониторинг, хранение и доступ к собираемым данным в соответствии с законодательством;

- контактные данные службы технической поддержки, ответственной за сервис eduroam.

6 Уведомления

1. Организация-участник eduroam (Провайдер идентификации и/или Сервис-провайдер) обязана предоставить Регистратору контактные данные двух уполномоченных технических представителей. При изменения контактной информации организация должна своевременно уведомить об этом Регистратора.
2. Провайдер идентификации должен назначить ответственное лицо по проблемам безопасности. Этим лицом может быть один из уполномоченных технических представителей.
3. Организации-участники eduroam (Сервис-провайдеры и Провайдеры идентификации) должны извещать Регистраторов о следующих инцидентах:
   - обнаруженных уязвимостях;
   - нарушениях правил использования сети или злоупотреблениях;
   - отказах сервиса;
   - изменениях в управлении доступом (запрет или разрешение доступа доменам или отдельным пользователям).

7 Статус документа, внесение изменений, ответственность и санкции

1. Настоящий регламент разработан и утвержден Национальной ассоциацией исследовательских и научно-образовательных электронных инфраструктур e-Arena.
2. Изменения в настоящем регламенте принимаются на основе консультаций с организациями-участниками Российской Удостоверяющей Федерации Eduroam.
3. Подключение RADIUS-сервера организации к национальной инфраструктуре eduroam рассматривается как согласие с требованиями настоящего Регламента. Любая научно-образовательная организация обязана в течение одного месяца после подключения к национальной инфраструктуре eduroam обязана подписать заявление о принятии настоящего Регламента или отключиться от инфраструктуры, если она не может в настоящее время принять данный Регламент.
4. В случаях, когда требуются немедленные действия для защиты целостности и безопасности сервиса eduroam, Оператор имеет право приостановить действие сервиса или ограничить его для тех организаций-участников, со стороны которых необходимы действия по устранению нарушений или уязвимостей. Оператор уведомляет участвующие организации об инцидентах, неисправностях и мерах по исправлению.
5. Оператор уведомляет по электронной почте уполномоченных технических представителей участвующей организации о любом техническом нарушении или инциденте, который требует принятия мер. В случае, если уведомление не будет своевременно обработано или в случае если инцидент может повлиять на безопасность и целостность eduroam, Оператор может заблокировать доступ организации к eduroam.
6. Сервис-провайдер может воспрепятствовать использованию своей сети для всех пользователей отдельного Провайдера-идентификации, настроив свой сервер авторизации на выдачу отказа заданному домену; в отдельных случаях Сервис-

провайдер может блокировать доступ конкретного пользователя.

7. Провайдер идентификации вправе ограничить доступ в eduroam отдельных своих пользователей настройками своего сервера аутентификации или удалением пользователя из базы данных.
8. Провайдер идентификации гарантирует, что его правила использования сети или иные административные правила, позволяют применить внутренние дисциплинарные взыскания к пользователю, нарушившему настоящий Регламент независимо от места и времени совершения нарушения.

Организация-участник:

_____

Участвует как

[ ] Сервис-провайдер (SP)

[ ] Провайдер идентификации (IdP) для следующих доменов:

Технический представитель 1:

Имя:_____

Эл.почта:_____

Тел.:_____

Технический представитель 2:

Имя:_____

Эл.почта:_____

Тел.:_____

Представитель по безопасности (Только для IdP):

[ ] приведенный выше технический представитель

[ ] указан ниже:

Имя:_____

Эл.почта:_____

Тел.:_____

Подписи и даты:

От организации-участника От Оператора/Регистратора