УДК 004.735

СПЕЦИФИКА ВНЕДРЕНИЯ EDUROAM В БГУИР

Романюк М.В., Лещенко Е.А., Савицкая Д.Г.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Марков А.Н. – старший преподаватель

Аннотация. Проведен анализ технических особенностей сети Eduroam и действующей беспроводной сети БГУИР. Установлено, что методы авторизации, реализованные университетом при подключении пользователей к сети Eduroam, в достаточной мере обеспечивают конфиденциальность вводимых данных и не нуждаются в совершенствовании. Выявлены недостатки реализации сети и предложены меры по ее совершенствованию.

Ключевые слова. беспроводная сеть университета, Eduroam, Wi-Fi, RADIUS

В современном мире всё тесно связано между собой посредством сетевых технологий. С каждым годом всё больше размываются границы между странами, становится меньше препятствий для коммуникации и международного сотрудничества и всё больше пользователей мобильных устройств, с которыми они могут перемещаться по всему миру. В связи с перечисленными выше факторами возникает потребность в безопасной международной Wi-Fi сети.

Глобальный сервис Eduroam (сокращение от роуминг для образования) позволяет пользователям (исследователям, преподавателям, студентам, научным сотрудникам) из участвующих в сервисе организаций безопасно получать доступ в Интернет из любого учреждения, имеющего подключение к системе Eduroam [1]. При этом сервис полностью бесплатен и для пользователей, и для учреждений, подключающихся к программе. Учреждения несут расходы исключительно на предоставление доступа в сеть интернет.

До внедрения Eduroam в БГУИР существовала гостевая Wi-Fi сеть «Guest», доступ к которой предоставлялся на ограниченное время, то есть DHCP сервер выдавал IP-адрес устройству на один час.

Несомненным преимуществом Eduroam является устранение необходимости создания временных учетных записей для посетителей БГУИР, которая возникала из-за постоянно растущего движения студентов и исследователей между учреждениями и странами. То есть сервис позволяет посетителям использовать одни и те же учетные данные для подключения к любой точке доступа Eduroam по всему миру [2].

Eduroam доступен в 106 странах мира. В некоторых из них сервис предоставлен не только в научных и образовательных учреждениях, но и на железнодорожных вокзалах, и в аэропортах. Со стороны нашей страны в сервисе принимают участие следующие организации: ОИПИ НАН Беларуси, БГУ, БГУИР, БНТУ, БГПУ им. М. Танка, ГГУ, ГрГУ, ПГУ [3].

С 1 января 2020 по 14 марта 2021 года к сети Eduroam на территории Республики Беларусь 44672 раза успешно подключались пользователи из других стран: Литвы, Латвии, Польши, Германии, Испании, Португалии, Исландии и многих других. За этот же период пользователи белорусских учреждений образования совершили 148230 успешных авторизаций в сети Eduroam, из них 27274 совершили студенты и работники БГУИР [4].

В БГУИР подключение к беспроводной сети Eduroam можно произвести в любом учебном корпусе. По состоянию на 14 марта 2021 года зону покрытия Wi-Fi в университете обеспечивают 92 беспроводные точки доступа. Проводится также модернизация беспроводной сети: например, на кафедре ПОИТ весной 2021 года планируется установка шести точек доступа с целью увеличения зоны покрытия беспроводной сети в 4 учебном корпусе.

Централизованно установить точки доступа Eduroam в общежитиях университета не представляется возможным ввиду требований законодательства Республики Беларусь, регламентирующего мощность излучения в местах постоянного и временного проживания.

С технической точки зрения Eduroam работает следующим образом: в каждой стране, которая внедряет данную технологию, есть сервера, хранящие информацию о пользователях. Эти сервера представлены RADIUS-сервером национального сегмента и RADIUS-серверами учреждений, подключенных к сервису. Аутентификация пользователей в любом сегменте Eduroam проводится их родительскими организациями с использованием тех же учётных данных и методов, что и при локальной аутентификации при нахождении в сети таковой, тогда как организация доступа к интернету лежит на посещаемом учреждении. Таким образом, роль системы заключается в переадресации учетных данных пользователей по иерархической системе RADIUS-серверов из посещаемой организации в родительскую, где они могут быть верифицированы.

Например, если пользователь, числящийся в системе БГУИР приехал в гамбургский университет и пытается там войти в сеть Eduroam, то запрос отправляется сначала на RADIUS-сервер гамбургского университета, оттуда – на сервер национального сегмента Германии, далее на сервер Eduroam верхнего уровня, потом на сервер национального сегмента Республики Беларусь и после этого на сервер БГУИР, который идентифицирует пользователя и отправляет обратно информацию об авторизации по той же цепочке серверов. Схема авторизации представлена на рисунке 1.

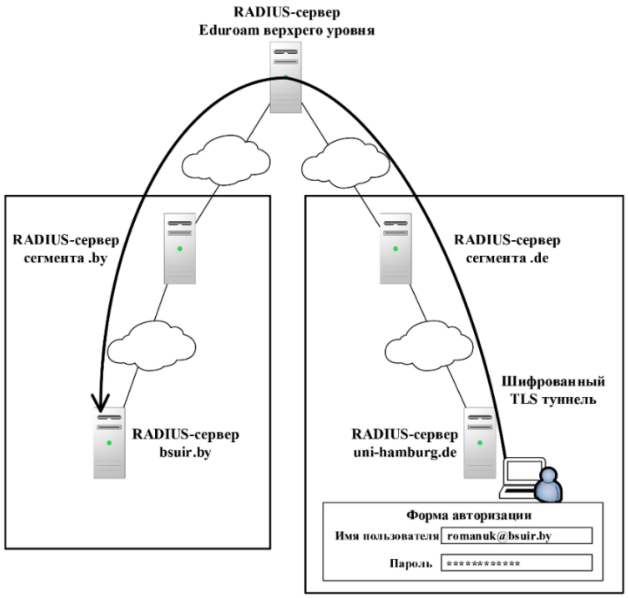

Рисунок 1 – Схема авторизации пользователя

Процедура, описанная выше, реализуется при помощи протоколов, описываемых в стандарте IEEE 802.1x. В этом стандарте определены механизмы аутентификации и авторизации пользователя на этапе подключения к сетевой среде передачи данных, ещё до предоставления доступа к таковой. То есть при использовании аутентификации по протоколу 802.1x в сети невозможно сделать ничего до того момента, пока от контролирующего RADIUS-сервера не придёт подтверждение, что подключающийся успешно аутентифицирован предъявлением действующего логина и пароля.

В БГУИР доступ к сети базируется на протоколе безопасности WPA2-EAP (Extensible Authentication Protocol), который является основой для инкапсуляции методов аутентификации и авторизации. Протокол прост и не требует от беспроводной точки доступа, к которой подключается пользователь, поддержки каких-либо специфичных методов аутентификации – она лишь передаёт EAP-запросы между клиентом и внешним сервером аутентификации RADIUS.

В качестве метода аутентификации, с учётом того, что запросы, содержащие логины и пароли пользователей, могут передаваться по цепочке неподконтрольных серверов в разных странах и юрисдикциях, выбран PEAP-MSCHAPv2. Согласно данному протоколу, при изначальном соединении между клиентом и сервером устанавливается шифрованное TLS соединение, требующее серверного сертификата. После установления TLS соединения в туннеле происходит авторизация по протоколу MSCHAPv2.

Получить доступ к сети, защищенной по протоколу PEAP-MSCHAPv2, можно только зная логин и пароль пользователя (взлом как таковой невозможен). Атаки типа перебора пароля или направленные на уязвимости в MSCHAP также не возможны или затруднены ввиду того, что EAP-канал «клиент-сервер» защищен шифрованным туннелем.

Таким образом, изучив особенности внедрения Eduroam в БГУИР можно сделать вывод о том, что этот сервис благоприятно влияет на качество обучения, позволяя студентам, в том числе и приехавшим по программам обмена, а также работникам получать бесплатный и, что важно, безопасный выход в интернет с любого устройства из любой точки университета.

Однако существуют и определённые особенности при работе с Eduroam. Во-первых, при первоначальной настройке подключения к сети Eduroam на устройствах с операционной системой Windows возникает необходимость создания подключения к беспроводной сети с заданием большого количества параметров вручную, а на Android – необходимость отключения проверки сертификатов, что у некоторых пользователей может вызвать трудности при отсутствии подробной инструкции. Во-вторых, с увеличением количества пользователей, подключенных к одной точке доступа, уменьшается зона ее покрытия. В-третьих, на точках доступа D-Link, установленных почти во всем университете, существует проблема с работой бесшовного роуминга, когда при переключении между точками доступа на некоторое время пропадает связь с сетью. Для решения данной проблемы необходима модернизация сети с использованием иных точек доступа. Например, на точках доступа высшего производительного и ценового сегмента Aruba, на основе которых построена сеть для администрации университета, данная проблема не наблюдается.

Список литературы

1. Координатор сервиса роуминговой аутентификации eduroam в Беларуси [Электронный ресурс]. – Режим доступа: https://eduroam.by/. – Дата доступа: 14.02.2021.

2. Роуминг для образования: БГУИР подключился к международной Wi-Fi-сети eduroam [Электронный ресурс] // Белорусский государственный университет информатики и радиоэлеткроники. – Режим доступа: https://www.bsuir.by/ru/news/101178-rouming-dlya-obrazovaniya-bguir-podklyuchilsya-k-mezhdunarodnoy-wi-fi-seti-Eduroam. – Дата доступа: 14.02.2021.

3. What is eduroam? [Electronic resource] // Eduroam. – Mode of access: https://www.eduroam.org/where/. – Date of access: 14.03.2020

4. Statistic data for country: by [Electronic resource] // Eduroam supporting services. – Mode of access: https://monitor.eduroam.org/f_ticks_stats.php?gtype=stats&country=by&obid=all&gtime=2020-01-01%2000:00:00::2021-03-13%2023:59:00. – Date of access: 14.03.2020

UDC 004.735

SPECIFICS OF IMPLEMENTATION EDUROAM IN BSUIR

Romaniuk M.V., Leschenko E.A., Savitskaya D.G.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Markov A.N.

Annotation. The analysis of the technical features of the Eduroam network and the current wireless network of BSUIR is carried out. It was found that the authorization methods implemented by the university when connecting users to the Eduroam network sufficiently ensure the confidentiality of the entered data and do not need to be improved. The drawbacks of the network implementation are revealed and measures for its improvement are proposed.

Keywords. university wireless network, Eduroam, Wi-Fi, RADIUS