ОРГАНИЗАЦИЯ WI-FI СЕТИ С ИСПОЛЬЗОВАНИЕМ ОТКРЫТЫХ РЕШЕНИЙ И ОТЕЧЕСТВЕННОГО ОБОРУДОВАНИЯ

BUILDING WI-FI NETWORKS USING OPEN SOLUTIONS AND RUSSIAN-MADE DEVICES

K. Kryazhenkov

Summary. The article discusses the issues of building a Wi-Fi network on on Russian-made devices. The choice of the solution is substantiated from the standpoint of interoperability, the logic diagram of the test prototype is described, and the results of testing in the test-bed. The solution is based Russian-made equipment and open source software, allowing to automate configuration management of wireless access point clusters, use the dual IPv4 / IPv6 stack, and control user access to a Wi-Fi network based on a digital fingerprint of user devices. In conclusion is possible to duplicate the considered solution and the tasks are outlined.

Keywords: Wi-Fi, import substitution, open source software, dual IPv4/IPv6 stack, digital fingerprint.

Кряженков Константин Геннадьевич
К.т.н., доцент, ФГБОУ ВО «МИРЭА — Российский технологический университет» (г. Москва)
konstantin@mirea.ru

Аннотация. В статье рассмотрены вопросы построения Wi-Fi сети на устройствах отечественного производителя. Обосновывается выбор решения с позиций функциональной совместимости, описывается логическая схема тестового прототипа и приведены результаты апробаций в пилотной зоне. Решение построено на отечественном оборудовании и свободном программном обеспечении, позволяя автоматизировать управление конфигурациями кластеров точек доступа, использовать дуальный стек IPv4/IPv6, контролировать доступ пользователей к Wi-Fi сети на основе цифрового отпечатка устройств. В заключении сделан вывод о возможности тиражирования рассмотренного решения и обозначены задачи развития.

Ключевые слова: Wi-Fi, импортозамещение, свободное программное обеспечение, стек IPv4/IPv6, цифровой отпечаток.

Формирование адаптивного образовательного пространства для мобильных пользователей требует наличия широкополосного сетевого доступа в любом месте и в любое время. Как следствие, повышаются требования к Wi-Fi сетям, по-прежнему актуальны вопросы безопасности, идентификации и ассоциации пользователей с устройствами, централизованного управления и мониторинга.

Угроза санкционных рисков ограничивает возможность построения новых проектов на аппаратно-программных решениях иностранных производителей. В этой связи интерес представляет переход к отечественному оборудованию и использованию свободного программного обеспечения при сохранении функциональной совместимости с уже эксплуатирующейся инфраструктурой. Эта проблематика рассмотрена в статье на примере опыта федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА — Российский технологический университет» (РТУ МИРЭА).

Организация Wi-Fi сети в РТУ МИРЭА направлена на обеспечение мобильности пользователей при доступе к единой электронной информационно-образовательной среды (ЭИОС) Университета, реализации всего потенциала концепции Bring Your Own Device (BYOD) [1, 2, 3], удовлетворения растущей востребованности сервисов класса OTT (Over The Top) [4, 5] и трансляции виртуальных рабочих столов VDI (Virtual desktop infrastructure) на мобильные устройства студентов и сотрудников [6, 7]. Все это требует надежного широкополосного беспроводного доступа в любой точке кампусной локации.

Несмотря на то, что к настоящему моменту Wi-Fi сеть Университета обслуживает более 200 точек доступа (ТД) диапазона 2,4 ГГц в дуальной архитектуре, где часть оборудования предоставлена Департаментом информационных технологий города Москвы, практика выявила потребность существенного наращивания зоны покрытия и установки дополнительных устройств.

Если ранее все установленное Wi-Fi оборудование и соответствующее программное обеспечение было представлено зарубежными производителями (преимущественно компании Cisco) [8], то сегодняшние реалии требуют активной реализации политики импортозамещения и перехода от проприетарного к отечественному или свободно распространяемому программному обеспечению. В этих условиях представляется актуальным вопрос обоснования и выбора соответствующих решений.

Перечислим основные требования к новым решениям. Применительно к ТД они состоят в следующем. ТД должны поддерживать протоколы PoE IEEE802.3af, 802.3at, а также быть совместимыми с prestandard Cisco

Po E. Наряду с этим, в них должны поддерживаться протоколы обнаружения соседних устройств, протокол RADIUS с функцией dynamic authorization service (DAS), а также использование одного идентификатора беспроводной сети SSID для спектра виртуальных локальных сетей (VLAN). Помимо этого, ТД должны уметь обеспечивать приоритезацию мультимедийного трафика, включая сервисы передачи голосовой информации по протоколу IP (VoIP) и поддерживать возможности многоадресатной рассылки в радиоэфире (multicast).

ТД обязательно должны взаимодействовать с системой идентификации пользователей для проверки их полномочий при доступе к Wi-Fi сети. Это обусловлено действующим законодательством Российской Федерации и внутренними нормативными документами РТУ МИРЭА. Основу системы идентификации в сети РТУ МИРЭА составляют решения с открытым исходным кодом, упростившие процессы интеграции с телекоммуникационным оборудованием, а также с корпоративным сервером каталогов. В качестве идентификационных данных для всех инфокоммуникационных сервисов Университета используется унифицированный идентификатор, совпадающий с адресом электронной почты обучающегося или сотрудника.

Для конкретизации требований и обоснования выбора решений была разработана программа и методика испытаний (ПМИ) функциональной совместимости беспроводного оборудования стандартов IEEE802.11 с используемыми в РТУ МИРЭА инфокоммуникационными решениями. В частности, ПМИ содержит 12 контрольных проверок для ТД:

1. Поддержка протоколов обнаружения соседних устройств CDP или LLDP;
2. Возможности сетевого управления по протоколам Telnet, SSH, SNMP;
3. Возможность работы в кластере или через контроллер;
4. Поддержка технологии 802.1q, в том числе для беспроводных интерфейсов;
5. Возможность использование одного SSID для разных VLAN;
6. Поддержка одновременной работы в двух диапазонах — 2,4 и 5 ГГц;
7. Поддержка аутентификации устройств пользователей по протоколу RADIUS;
8. Наличие системы мониторинга радиоэфира и автоматической адаптации к уровню интерференции;
9. Наличие системы обнаружения несанкционированных ТД;
10. Поддержка многоадресатной рассылки в радиоэфире;
11. Реализация функций качества обслуживания в радиоэфире для голосового трафика;
12. Централизованное обновление операционной системы (JC) ТД, резервное копирование и восстановление файлов конфигурации и ОС.

При выборе нового оборудования учитывался факт наличия у производителя устройств, включенных в реестр телекоммуникационного оборудования российского происхождения Минпромторга [9]. Анализ этого реестра показал, что на момент 2018 года, номенклатурой оборудования представлен отечественный производитель — ООО «Предприятие Элтекс» (https://eltex-co.ru/). Важным преимуществом этого производителя является наличие в реестре не только ТД, но и коммуникационного оборудования, с которым они работают. Отметим, что ранее по результатам соответствующего тестирования были выбраны и имплементированы в сетевую инфраструктуру Университета коммутаторы уровня агрегации Eltex MES5324, MES5312, MES3324F и уровня доступа Eltex MES2324P, MES2348P. Вместе с унаследованным оборудованием Cisco они обеспечивают функционирование магистральных каналов с полосой от 10 до 80 Гбит/с, обслуживая несколько тысяч пользователей. Применительно к ТД всем требованиям ПМИ удовлетворяют модели Eltex WEP-2ac и WEP-2ac Smart, причем последняя поддерживает технологию интеллектуальных антенн. Отметим, что в последнее время наблюдается расширение номенклатуры сетевого оборудования отечественного производства, что увеличивает возможности выбора.

Этапу масштабного внедрения предшествовала окончательная проверка выбранных решений. Для этого был разработан и развернут тестовый прототип Wi-Fi сети, логическая схема которого представлена на рисунке 1.

Прототип состоит из следующих функциональных модулей — Кластер ТД, Модуль управления ТД, Модуль управления доступом к сети, Сетевые сервисы и Пользователи. Рассмотрим их более подробно.

Кластер ТД объединяет в своем составе несколько ТД, имеющих идентичную конфигурацию. Ему назначается единый IP–адрес управления, который связан с ТД, имеющей больший приоритет в кластере. На данной ТД производится конфигурация кластера, включая режим работы беспроводной системы обнаружения вторжений (IDS). Система IDS необходима для выявления потенциально возможных фактов несанкционированного размещения ТД в кампусной сети. Кластер также позволяет упростить частотное планирование за счет периодического мониторинга радиоэфира и переназначения радиоканалов на ТД в кластере.

Большое число ТД и созданных на их основе кластеров требует существенных усилий при развертывании и обслуживании. Снизить эти затраты позволяет специально

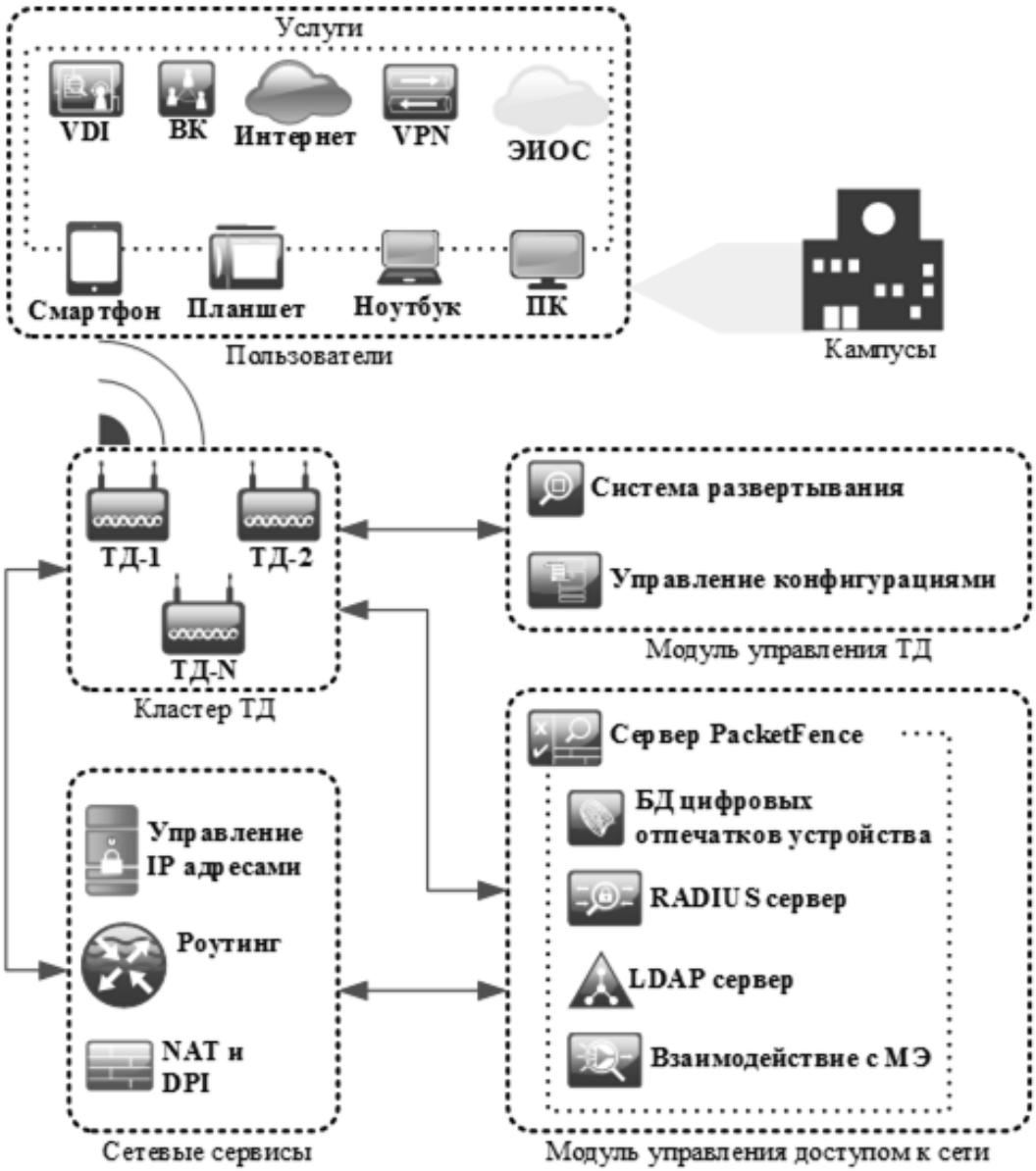

Рис. 1. Логическая схема прототипа беспроводной сети

разработанный при участии автора Модуль управления ТД, написанный на языке Python. Этот модуль выполняет задачу развертывания и управления конфигураций всех ТД. После того, как новая ТД была подключена к сети и получила по протоколу DHCP сетевой адрес на интерфейс управления, система развертывания обнаруживает такую ТД и производит ее конфигурацию в соответствии с правилами, определенными администратором Wi-Fi сети в шаблоне конфигурации ТД. После настройки ТД система управления конфигурациями запрашивает конфигурационный файл ТД и размещает его в репозитории конфигураций. Последний обновляется после внесения изменений в конфигурацию ТД. Сохраненная в репозитории конфигурация может быть использована для восстановления параметров системой развертывания в случае утраты конфигурации на ТД.

В ТД моделей WEP-2ac и WEP-2ac Smart используется ОС Linux и свободное программное обеспечение hostapd (https://w1.fi/hostapd/) для создания виртуальных точек доступа (VAP). Таким образом, становится возможным после идентификации пользователя организовать мапирование одного SSID в несколько VLAN. Это позволяет сделать процесс применения полномочий пользователей более гибким и безопасным. Так, пользователь, используя только один SSID прозрачно переключается в разрешенную ему сеть. Причем, самостоятельно пользователь не сможет произвести настройку подклю-

чения к той или иной VLAN, это делается динамически по протоколу RADIUS. Помимо этого, ТД поддерживают конфигурацию оверлейной сети посредством сервиса OTT, что может в будущем использоваться для формирования выделенных сетевых сегментов для проектных или научных групп.

Для идентификации пользователя и предоставления ему услуг используются Модуль сетевые сервисы и Модуль управления доступом к сети. После ассоциации с ТД сетевой сервис DHCP назначает на пользовательское устройство сетевые реквизиты для доступа к серверу Network Access Control (NAC). В качестве системы NAC использовано свободное ПО Packetfence (https://packetfence.org/), которое предварительно было модернизировано: проведена локализация пользовательских сообщений, доработан модуль captive portal, а также разработаны модули для поддержки ТД российского производителя ООО «Предприятие Элтекс» и скорректирован модуль работы со стеком протокола IPv6. Отметим, что сервис DHCP, NAC и сервис маршрутизации работают совместно: сервер DHCP назначает адрес на оконечное устройство пользователя, маршрутизатор обновляет у себя ARP–запись, а NAC запоминает параметры связки «MAC–адрес пользователя: IP–адрес пользователя: IP-адрес ТД». Этот механизм препятствует подмене аппаратных и IP–адресов, что может являться причиной компрометации NAC.

Дополнительно для однозначной идентификации устройства пользователя применяется механизм определения цифровых отпечатков устройств. Цифровой отпечаток — это информация, собранная об абонентском устройстве для целей дальнейшей идентификации.

Получение цифрового отпечатка происходит скрытым способом на основе DHCP–опций, которые позволяют определить типы операционных систем и вид устройства пользователя. Полученные данные сравниваются с результатами выгрузки с официального сайта fingerbank.org. Информация об устройстве пользователя связывается с его IP–адресом, что уменьшает возможность компрометации NAC. Поэтому если один из параметров (MAC–адрес или цифровой отпечаток устройства) изменится, то NAC произведет блокировку данного устройства и сообщит об этом администратору беспроводной сети.

Аутентификация и авторизация пользователя производятся посредством специализированной веб–страницы. Вне зависимости от ОС (Linux, MS Windows, Mac OS, Android и т.д.) пользовательского устройства доступ к данной странице происходит автоматически, либо после ввода в строке поиска веб–браузера любого URL–адреса. На предоставленной странице аутентификации пользователь вводит свой логин и пароль. В качестве логина используется адрес электронной почты в домене mirea.ru (для сотрудников) или edu.mirea.ru (для обучающихся). Гостевой доступ планируется реализовать с помощью единой системы идентификации и аутентификации (ЕСИА), а также других доверенных способов, позволяющих однозначно идентифицировать абонента Wi-Fi сети.

В случае с сотрудниками и обучающимися Университета применяется следующий алгоритм. Система NAC запрашивает RADIUS–сервер для получения информации о результатах проверки пользователя и возможностей его подключения к сети. RADIUS–сервер взаимодействует с корпоративным LDAP–сервером для поиска информации о пользователе и его пароле. В случае успешной проверки RADIUS–сервер сообщает на NAC возможности сетевого подключения, включая идентификатор VLAN. NAC–сервер отправляет на ТД сообщение об отключении пользователя и его повторном подключении к тому же SSID, но производит мапирование его в другую VLAN, обеспечивающую доступ к услугам. Такой подход позволяет прозрачно поместить пользователя в необходимый сетевой сегмент без изменения SSID.

В назначенной VLAN на пользовательское устройство по протоколу DHCP передаются сетевые реквизиты для моделей протокола IPv4 и IPv6. Режим использования IPv6–адресов SLAAC исключен, т.к. не позволяет однозначно идентифицировать устройство пользователя. Таким образом, пользователи с ОС Android не могут использовать двойной стек, т.к. модель протокола IPv6 на данной ОС поддерживает только SLAAC. Однако, все услуги им будут полностью доступны по IPv4, а все требования по идентификации будут соблюдены.

Компонент взаимодействия с межсетевым экраном (МЭ) обеспечивает фиксацию сессий пользователей. Информация о пользователе, IPv4 и IPv6–адресах, связанных с устройством, передается на МЭ, что позволяет сохранить запись в системном журнале о сессии пользователя, в том числе, при глубоком анализе пакетов (DPI). DPI применяется для ограничения взаимодействия пользователя с нежелательным контентом из сети Университета. Нежелательный контент ранжируется по категориям, которые могут быть применены к конкретному пользователю или группе пользователей. Категории нежелательного контента определяются как законодательными требованиями, так и внутренними нормативными актами. Помимо этого, идентификация пользователя на МЭ позволяет сохранить информацию о нем при трансляции сетевых адресов (NAT). Информация о пользовательских сессиях передается по протоколу SYSLOG на специализированный сервер, где сохраняется для будущего анализа вопросов безопасности.

Рис. 2. Распределение ОС пользовательских устройств

DHCP Fingerprint	Total
iOS	1.68 GB
Android OS	659.80 MB
Windows OS	13.25 MB
Mac OS X or macOS	7.69 MB
Audio, Imaging or Video Equipment	0.84 MB
Operating System	768.29 KB
Unknown Fingerprint	635.61 KB
Linux OS	85.77 KB
Phone, Tablet or Wearable	45.99 KB

Рис. 3. Объем потребленного трафика

Campus-D-fw-2 : 2019/05/01 09:24:00 - 2019/06/30 09:24:00

App Category	App Sub Category	Risk	Sessions
unknown	unknown	1	25.47 k
general-internet	internet-utility	2	72.13 k
collaboration	voip-video	4	24.38 k
networking	infrastructure	4	66.72 k
networking	infrastructure	2	1.96 k
networking	encrypted-tunnel	4	22.10 k
general-internet	internet-utility	4	8.77 k
collaboration	social-networking	4	3.11 k
networking	infrastructure	1	2.50 k
collaboration	email	4	1.13 k

Рис. 4. Типы используемых приложений

Описанный выше тестовый прототип прошел апробацию на пилотных зонах. Каждая пилотная зона состоит из двух кластеров, суммарно содержащих 7 отечественных ТД. Кластеры разнесены по кампусам и взаимодействуют с NAC, установленном в ядре сети РТУ МИРЭА.

Период апробации был выбран в зачетную и экзаменационную сессии весеннего семестра 2019 года. За данный период в сервисе зарегистрировалось более 250 устройств пользователей, причем, доминирующее большинство ОС это MacOS, рисунок 2.

Как видно из рисунка 2, доминируют устройства компании Apple, а неопределенные по методу DHCP fingerprint устройства составляют менее 6% от общего числа. Таким образом, в пилотных зонах подтверждена возможность использования дуального стека моделей протокола IP, что существенно снизит нагрузку на МЭ, т.к. IPv6–адреса не нуждаются в преобразовании.

На рисунке 3 приведена статистика потребления трафика пользовательскими устройствами в разрезе ОС, а на рисунке 4 типы использованных приложений в пилотной зоне.

Данные на рисунках 3, 4, в частности, показывают, что в период апробации пилотная зона использовалась пользователями для таких критичных к качеству обслуживания приложений как голосовые вызовы по технологии VoWiFi и видеоприложения.

Результаты апробаций рассмотренного решения показали, что современное отечественное оборудование и программные средства на открытом коде позволяют решить задачу импортозамещения при построении кампусных Wi-Fi сетей. Описанный выше тестовый прототип легко встраивается в существующую сетевую инфраструктуру, является масштабируемым и обеспечивает выполнение ключевых требований по функциональности и безопасности. Он может рассматриваться как тиражируемое решение, позволяющее минимизировать затраты на развертывание и сопровождение беспроводных сетей.

Ближайшие задачи развития состоят в интеграции системы идентификации в Wi-Fi сети с сервисами ЕСИА и Eduroam. Наряду с этим, планируется добавление новых сервисов в Wi-Fi сеть, таких как передача многоадресатной рассылки и реализация защищенных соединений на основе EAP-TLS. Для этих целей потребуется модернизация системы контроля доступа пользователей к Wi-Fi сети и разработка механизмов предоставления сертификатов пользователей, а также их использовании на мобильных устройствах под управлением iOS и Android.

ЛИТЕРАТУРА

1. Gökçe, K. G., & Dogerlioglu, O. (2019). "Bring your own device" policies: Perspectives of both employees and organizations. Knowledge Management & E-Learning, 11(2), pp. 233–246.— Режим доступа: https://www.kmel-journal.org/ojs/index.php/online-publication/article/view/411
2. Mohamed Al Askar, Kathy Ning Shen. Understanding Bring Your Own Device (BYOD) and Employee Information Security Behaviors from A Work-Life Domain Perspective. Twenty-second Americas Conference on Information Systems, San Diego, 2016.— Режим доступа: https://pdfs.semanticscholar.org/0b91/b2bcd72ab98678751b5b0847cdfce4cbab50.pdf
3. Madhavi Dhingra. Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). Procedia Computer Science, Volume 78, 2016, pp. 179–184 — Режим доступа: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&uact=8&ved=2ahUKEwjcsses8IHlAhVn16YKHS0ZAvMQFjAJegQICRAC&url=https%3A%2F%2Fcyberleninka.org%2Farticle%2Fn%2F539053.pdf&usg=AOvVaw3SAUZe5iI4RVVKl39b_JXN
4. Деарт В.Ю., Кожухов И. С. Исследование параметров качества обслуживания (QoS), определяющих качество восприятия пользователем (QoE) потокового видео при передаче через Интернет // T-Comm — Телекоммуникации и транспорт, 2013.— № 7.— С. 28–31.
5. Joshi Sujata, Sarkar Sohag, Dewan Tanu, etc. Impact of Over the Top (OTT) Services on TelecomService Providers — ndian Journal of Science and Technology, Vol 8(S4), 145–160, February 2015.— Режим доступа http://www.indjst.org/index.php/indjst/article/viewFile/62238/48529
6. Двоеглазов Д.В., Дешко И. П., Кряженков К. Г., Тихонов А. А. Опытный полигон DaaS в МГТУ МИРЭА // Академический форум корпорации EMC: сборник тезисов докладов участников конференции, 20–25 октября 2014 г., г. Москва / Факультет ВМК МГТУ имени М. В. Ломоносова.— М.: МАКС Пресс, 2014.— С. 99–102.
7. Двоеглазов Д.В., Дешко И. П., Кряженков К. Г., Тихонов А. А. Инфраструктура виртуальных рабочих столов на открытых программных продуктах [Электронный ресурс] // Интернет-журнал «Науковедение».— М.: 2015.— т. 7.— № 4(29).— Режим доступа: http://naukovedenie.ru/PDF/37TVN415.pdf
8. Кряженков К.Г, Тихонов А. А. Система беспроводного доступа в корпоративную сеть МИРЭА // Современные информационные технологии в управлении и образовании. Сборник научных трудов. М: ФГУП НИИ «ВОСХОД», МИРЭА, 2004 г.— С. 65–68.
9. Реестр телекоммуникационного оборудования, произведенного на территории Российской Федерации, которому присвоен статус телекоммуникационного оборудования российского происхождения [Электронный ресурс].— Режим доступа: http://minpromtorg.gov.ru/opendata/7705596339-tkorpregister/

Журнал «Современная наука: актуальные проблемы теории и практики»