УДК 004.056

Аржаков А.В., Атавина А.В., Зарешин С.В., Сильнов Д.С.

Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия

АНАЛИЗ ЗАЩИЩЕННОСТИ ОБЩЕДОСТУПНЫХ WI-FI СЕТЕЙ НА УЛИЦАХ МОСКВЫ

АННОТАЦИЯ

Исходя из возрастающей популярности использования Wi-Fi сетей, в статье рассматриваются проблемы уязвимости Wi-Fi сетей, проблемы связанные с безопасностью использования беспроводных сетей и доступа к ним. Сравниваются различные методы шифрования и аутентификации, определяются основные параметры для настройки сетей с безопасным доступом. Также приводится статистика использования Wi-Fi сетей в центральном районе Москвы, степень их защищенности и доступности.

КЛЮЧЕВЫЕ СЛОВА

Беспроводные сети; Wi-Fi; Интернет; протокол шифрования; способ аутентификации; защищенность; уязвимость; информационная безопасность; перехват информации.

Arzhakov A.V., Atavina A.V., Zareshin S.V., Sil'nov D.S.

National Research Nuclear University MEPHI, Moscow, Russia

ANALYSIS OF SECURITY OF PUBLIC ACCESS TO WI-FI NETWORKS ON THE MOSCOW STREETS

ABSTRACT

According to the growing popularity of using Wi-Fi networks, the article describes the vulnerability of Wi-Fi networks, the problems associated with the safety of using wireless networks and access to them. Compare different methods of encryption and authentication, identifies the main options for configuring secure access to networks. It also provides statistics on the use Wi-Fi networks in the central district of Moscow, the degree of security and availability.

KEYWORDS

Wireless networks; Wi-Fi; Internet; 802.11; protocol of encryption; method of authentication; security; vulnerability; information security; interception of data.

В настоящее время интернет занимает лидирующие позиции по получению информации. С его помощью человечество может получать образование, обмениваться мыслями и мнениями с другими пользователями сети, пересылать различную информацию. Существуют два способа передачи данных: проводной и беспроводной. Преимуществом проводного способа является высокая скорость работы и повышенная физическая защищенность канала передачи данных.

Беспроводной способ является более мобильным. Но в тоже время стабильная передача данных и одновременная работа в одном месте множества беспроводных точек вызывает коллизии, а именно, накладывание нескольких передатчиков друг на друга, вследствие чего суммарный сигнал становится искаженным. Эта проблема препятствует правильной передаче данных по сети [1]

Wi-Fi сети за последние несколько лет получили огромное распространение. Все больше ведущих организаций мира активно используют развивающуюся технологию Wi-Fi и предоставляют Wi-Fi услуги своим клиентам. Множество различных устройств последнее время производятся со встроенной поддержкой Wi-Fi, будь то мобильные телефоны, планшеты, ноутбуки или любое другое устройство из всего многообразия различных гаджетов. Для подключения к беспроводной сети лишь необходимо находиться в радиусе её действия. Действия по определению Wi-Fi сетей и настройки необходимых параметров происходят автоматически. Устройство, находящееся в радиусе действия нескольких Wi-Fi сетей, может подключаться к той или иной точке доступа либо по выбору пользователя, либо автоматически – к сети, которая имеет самый мощный уровень сигнала. Также происходит периодическая проверка наличия точки доступа с лучшим

уровнем сигнала.

Беспроводная сеть Wi-Fi обладает следующими преимуществами, главными из которых являются:

- организация, использование и расширение сети без использования кабеля;
- возможность динамического изменения топологии сети;
- возможность использования одной точки доступа несколькими пользователями;
- простота в проектировании и реализации.

В то же время беспроводная сеть обладает и некоторыми недостатками, одним из которых является зависимость скорости соединения от наличия различных преград и количества подключенных устройств, а также уязвимость сети в части безопасности в связи с облегчённым физическим доступом к сигналу.

С каждым днем число пользователей, которые пользуются устройствами с беспроводным выходом в Интернет, непрерывно растет. Аналогично растет и количество злоумышленников, всячески пытающихся получить доступ к данным других пользователей и воспользоваться ими в личных целях. Так, подключение к Wi-Fi сети, со слабыми настройками безопасности, является рискованным: передаваемые данные, могут быть доступны посторонним лицам, вследствие чего вся конфиденциальная информация может стать открытой для злоумышленников. Для перехвата всех необходимых данных достаточно находиться в зоне действия сети Wi-Fi, в которой непосредственно находится электронное устройство. Целью злоумышленников может быть как нарушение каждой из составляющей данных: конфиденциальности, доступности, целостности, так и перехват информации для дальнейшего использования в личных целях.

Необходимо также отметить, что требования к повышенной защищенности Wi-Fi сетей ужесточаются и в связи с возрастанием террористических угроз. В частности, с января 2016 года, согласно Постановлениям Правительства [2, 3] идентификация пользователей и их устройств в публичных Wi-Fi сетях становится обязательной.

Подход к выявлению уязвимостей можно разделить на несколько частей. Прежде всего, необходимо понять, какие параметры беспроводных точек влияют на их уязвимость. Что конкретно может быть изменено в настройках для получения наиболее безопасной точки доступа. Что следует знать пользователю при желании подключиться в общественном месте к Wi-Fi сети. Далее, после выявления теоретических сведений о беспроводных сетях необходимо произвести сбор информации и затем обработать полученные данные с последующим их исследованием и обоснованием.

Для того чтобы выявить уязвимости, необходимо разобраться в параметрах беспроводных сетей. Постоянно растут новые способы борьбы с несанкционированным получением данных, появляются новые средства защиты. Таким образом, необходимо проанализировать основные принципы работы и организации беспроводных сетей, чтобы понять их уязвимости, исследовать масштаб проблемы, чтобы в дальнейшем определить объем незащищенных, либо использующих небезопасные протоколы шифрования Wi-Fi точек доступа.

Безопасная система по определению должна обладать тремя свойствами: конфиденциальности, доступности и целостности. Свойство конфиденциальности гарантирует пользователю, что его секретные данные будут доступны только ему либо группе лиц, которым доступ к ним разрешен. Свойство доступности говорит о том, что авторизованные пользователи в любой момент времени имеют право получить доступ к данным. Свойство целостности подразумевает неизменность параметров и характеристик, заданных при конфигурации устройства. Это свойство необходимо, поскольку от него зависит защита конфиденциальности Wi-Fi сети. Благодаря этому свойству злоумышленник не может изменить параметры настройки устройства, что могло бы привести к изменению очередности работ и даже к выводу устройства из строя. Для того чтобы обеспечить устройства, подключенные к беспроводной сети безопасностью, необходимо в первую очередь понимать, какие параметры обеспечивают конфиденциальность, целостность и доступность данных.

В первую очередь немаловажным параметром любой беспроводной сети является тип шифрования. Одним из важных аспектов при передаче данных по сети является шифрование трафика, так как для перехвата информации, передаваемой по беспроводной сети, не нужно физического воздействия, а достаточно просто «слушать» канал и перехватывать интересующую информацию.

Сейчас наиболее распространены несколько видов шифрования:

- NONE – открытый вид шифрования, данные передаются без какого-либо ключа, каждый желающий может получить доступ к данной беспроводной сети («небезопасная сеть»). В большинстве случаев используется для гостевого доступа;

- WEP – основанный на алгоритме RC4 шифр с разной длиной статического или динамического ключа (64 или 128 бит). Его алгоритмы выложены в открытом доступе, что позволяет злоумышленникам собирать статистику до тех пор, пока не будет получен ключ шифрования. Сеть, основанная на таком способе шифрования, не является безопасной. WEP — это небезопасный и функционально устаревший стандарт;
- TKIP – данный способ шифрования является усовершенствованным способом WEP. К нему добавлены дополнительные проверки на безопасность и защита. Ключи шифрования имеют длину 128 бит и генерируются по сложному алгоритму, а общее количество возможных вариантов ключей достигает сотни миллиардов, и меняются они очень часто. Но TKIP является устаревшим, он обладает более низким уровнем безопасности, чем стандарт AES, который приходит ему на замену;
- CCMP – наиболее совершенный алгоритм с дополнительными проверками и защитой. Это новый метод защиты при беспроводной передаче данных. Обеспечивает более надежный метод шифрования по сравнению с TKIP. CCMP выбирается в качестве метода шифрования, когда необходима повышенная безопасность данных.

Также для выявления сетей с небезопасным доступом, надо рассмотреть взаимодействия точки доступа и беспроводного клиента, по-другому называемые способы аутентификации:

- OPEN – открытая сеть. Все подключаемые устройства авторизуются автоматически;
- WPA – Personal - Данный режим подходит для большинства домашних сетей. Когда на беспроводную точку доступа устанавливается пароль, он должен вводиться пользователями каждый раз при подключении к сети Wi-Fi;
- WPA – Enterprise - Данный режим предоставляет необходимую в рабочей среде защиту беспроводной сети. Данный режим сложнее в настройке и предлагает индивидуальное и централизованное управление доступом к вашей сети Wi-Fi. Когда пользователи попытаются подключиться к сети, им понадобится предоставить свои учетные данные для аутентификации.

WPA2 – это вторая версия набора алгоритмов и протоколов, обеспечивающих защиту данных в беспроводных сетях Wi-Fi. Как предполагается, WPA2 должен существенно повысить защищенность беспроводных сетей Wi-Fi по сравнению с прежними технологиями. Новый стандарт предусматривает, в частности, обязательное использование более мощного алгоритма шифрования AES и аутентификации 802.1X. Протоколы WPA2 работают в двух режимах аутентификации: персональном (Personal) и корпоративном (Enterprise):

- WPA2 – Personal - на данный момент является самой надежной формой защиты, предлагаемой устройствами Wi-Fi, и ее рекомендуется использовать для всех целей. В режиме WPA2-Personal из введенной открытым текстом парольной фразы генерируется 256-разрядный ключ PSK (PreShared Key). Ключ PSK совместно с идентификатором SSID (Service Set Identifier) используются для генерации временных сеансовых ключей PTK (Pairwise Transient Key), для взаимодействия беспроводных устройств. Как и статическому протоколу WEP, протоколу WPA2-Personal присуще определенные проблемы, связанные с необходимостью распределения и поддержки ключей на беспроводных устройствах сети, что делает его более подходящим для применения в небольших сетях из десятка устройств, в то время как для корпоративных сетей оптимален WPA2-Enterprise;
- WPA2 – Enterprise - В режиме WPA2-Enterprise решаются проблемы, касающиеся распределения статических ключей и управления ими, а его интеграция с большинством корпоративных сервисов аутентификации обеспечивает контроль доступа на основе учетных записей. Для работы в этом режиме требуются такие регистрационные данные, как имя и пароль пользователя, сертификат безопасности или одноразовый пароль, аутентификация же осуществляется между рабочей станцией и центральным сервером аутентификации [4].

На примере центра Москвы, как района, наиболее насыщенного Wi-Fi сетями, представляет интерес выполнить анализ уязвимостей беспроводных сетей и оценить существующее на сегодняшний день распределение сетей по типу шифрования и способам аутентификации.

Для анализа уязвимостей беспроводных сетей в центральной части Москвы был произведён сбор информации. В формулируемом подходе он заключается в следующем. При помощи необходимого оборудования, а именно, GPS устройства (GlobalSat BU – 353s4), позволяющего точно оценить местоположение беспроводной точки доступа, были получены координаты Wi-Fi сетей в центре Москвы, согласно заданному заранее маршруту. В него были включены центральные улицы, переулки, набережные, проезды и площади с большим разнообразием общественных мест, что и позволило в дальнейшем провести анализ

общедоступных Wi-Fi сетей города Москвы. GPS приемник IV поколения представляет собой устройство с USB интерфейсом на чипсете SiRF STAR IV, обеспечивающий высокое качество и скорость определения координат. В одном корпусе присутствуют приёмник и активная антенна. Магнитное основание служит для крепления GPS – приёмника в любом удобном месте, обеспечивающем качественный прием сигнала спутниковой навигационной системы. К аппаратным характеристикам GlobalSat BU – 353s4 можно отнести следующие [5]:

- частота - L1, 1575.42 МГц;
- количество каналов - 48, "All-in-View", -163 dBm.

Точность:

- определение скорости - 0.1 м/сек, 95% (селективный доступ отключён);
- определение времени - 1 мкс, синхронизация по атомным часам GPS-спутников;
- датум - WGS-84.

Время захвата позиции:

- обновление данных - 0.1 сек;
- горячий старт - 8 сек., в среднем;
- холодный старт - 35 сек., в среднем;
- теплый старт - 35 сек., в среднем.

Последовательный порт:

- формат – ASCII;
- протоколы GPS - NMEA 0183 (вер. 3.0) (по умолчанию)/Двоичный SiRF;
- данные GPS - Двоичный SiRF: позиция, скорость, высота, статус, управление; NMEA 0183 (вер. 3.0): GGA, GSA, GSV, RMC (GLL, VTG - опционально);
- скорость передачи - Изменяется программно. По умолчанию: NMEA - 4800 б/с, двоичный SiRF - 19200 б/с.

Питание:

- напряжение питания - 4,5 В ~ 5,5 В, постоянный ток (от USB-порта);
- потребляемый ток - 55 мА.

Ограничения:

- максимальная высота - До 18000 м (60000 футов);
- максимальная скорость - До 515 м/с (1000 узлов);
- максимальное ускорение - До 4g.

Характеристики окружающей среды:

- температура эксплуатации - - 40° ~ + 85°C;
- влажность - До 95%, неконденсированная.

Физические характеристики:

- габариты - 53 мм (диаметр) x 19.2 мм (высота);
- длина кабеля – 1,5 м;
- масса – 69г.

Также в работе был использован двухдиапазонный усилитель беспроводного сигнала, при помощи которого обеспечивалась возможность максимального всенаправленного покрытия для беспроводной сети. Аппаратные характеристики TP-LINK AC1200 следующие [6]:

- диапазоны частот беспроводной связи – 2,4 ГГц и 5 ГГц (по одному каналу на прием и передачу). Что позволяет улучшить возможности беспроводного адаптера настольного компьютера или ноутбука;
- стандарт Wi-Fi – 802.11ac (+ поддержка более ранних стандартов 802.11a/b/g/n);
- мощность приемопередатчиков сигнала – 20 dBm (2,4 ГГц) и 20 dBm (5 ГГц);
- скорость приема/передачи: канал 5 ГГц – 867 Мбит/сек, канал 2,4 ГГц – 300 Мбит/сек;
- максимальная скорость соединения – 1200 Мбит/сек;
- зона покрытия – 1000 кв. метров;
- режимы работы – репитер, точка доступа;
- антенны – 2 штуки, несъемные;
- блок питания – внутренний;
- способы питания – кабель USB 3.0;
- материал корпуса – глянцевый белый пластик;
- габариты– 90*68*15 мм.

Общий вид используемого в работе стенда представлен на рисунке 1.

Рисунок 1 – Оборудование для поиска уязвимых Wi-Fi точек

Полученные при проходе маршрута данные заносились в таблицу при помощи установленной программы VIistumbler. Пример использования программы проведен на рисунке 2. Автоматически были определены следующие параметры пойманных беспроводных точек: идентификатор и название беспроводной сети (рабочее системное имя); MAC адрес устройства (физический адрес точки доступа); производитель точки доступа; максимальный уровень пойманного сигнала; показатель уровня принимаемого сигнала (мощность Wi-Fi сигнала); тип шифрования; способ авторизации; канал, на котором работает устройство; координаты пойманной точки; время и дата.

Последняя часть работы – обработка полученных данных. Для более полного понимания собранной информации и дальнейшего составления статистики на её основе, удобнее всего обрабатывать данные при помощи соответствующего синтаксического анализатора. С его помощью занесенные в таблицу EXCEL данные должны быть преобразованы в SQL-скрипт для последующего их занесения в базу данных. Из всей полученной информации, посредством запросов, можно получать интересующие в конкретный момент времени данные из всего объёма информации.

После проведения аналитической части работы было проанализировано 2357 сетей, относящихся к 29 улицам, переулкам, набережным, площадям и проездам в центральной части Москвы, в районе кремлевского кольца. Для более наглядного расположения точек была использована программа Google Earth, на карте которой обозначены все пойманные Wi-Fi сети, (они представлены на рисунке 2).

Рисунок 2 – Нанесенные точки доступа на GOOGLE EARTH

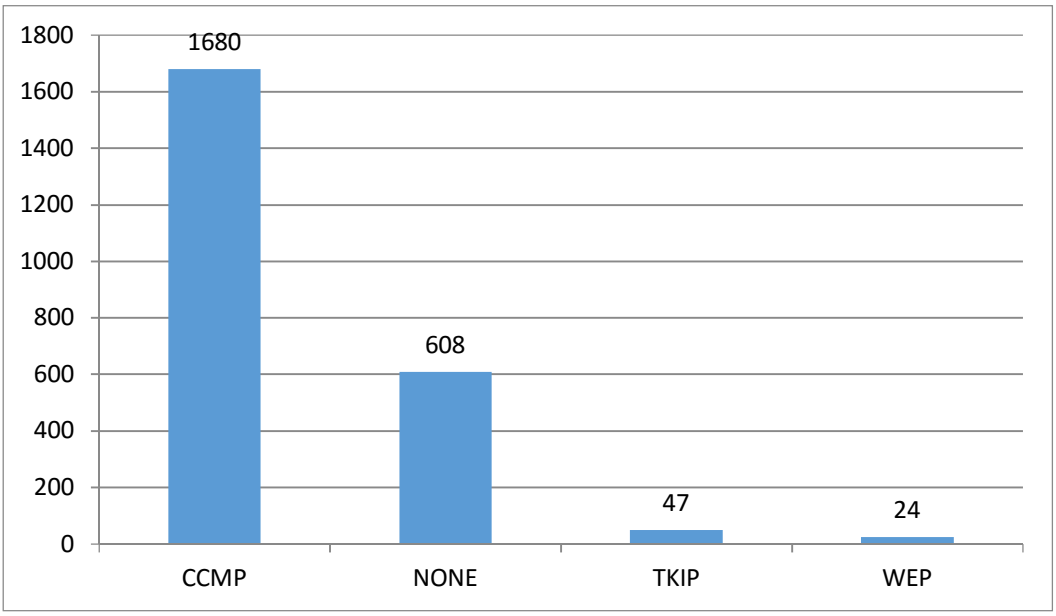

Рисунок 3 - Распределение беспроводных сетей по типу шифрования

В результате анализа полученных данных была выполнена оценка защищенности беспроводных точек в центре Москвы. Полученные оценки были основаны на анализе типа шифрования и способа аутентификации. На приведенных ниже гистограммах видно, что по типу шифрования Wi-Fi сети в центре Москвы в основном защищены от атак злоумышленников. Но, несмотря на то, что около 71% всех проверенных беспроводных точек используют надежный метод шифрования CCMP, оставшиеся 29%, используют менее защищенные способы, такие как: TKIP, WEP или, вообще, открытый вид шифрования (рисунок 3). Также можно сделать вывод, что беспроводные сети в центре Москвы в основном защищены от угроз и по способу аутентификации: наиболее надежной формой защиты пользуются подавляющее количество – 65%, но также стоит отметить, что 27% всех устройств – это открытые сети, не требующие авторизации пользователей (рисунок 4).

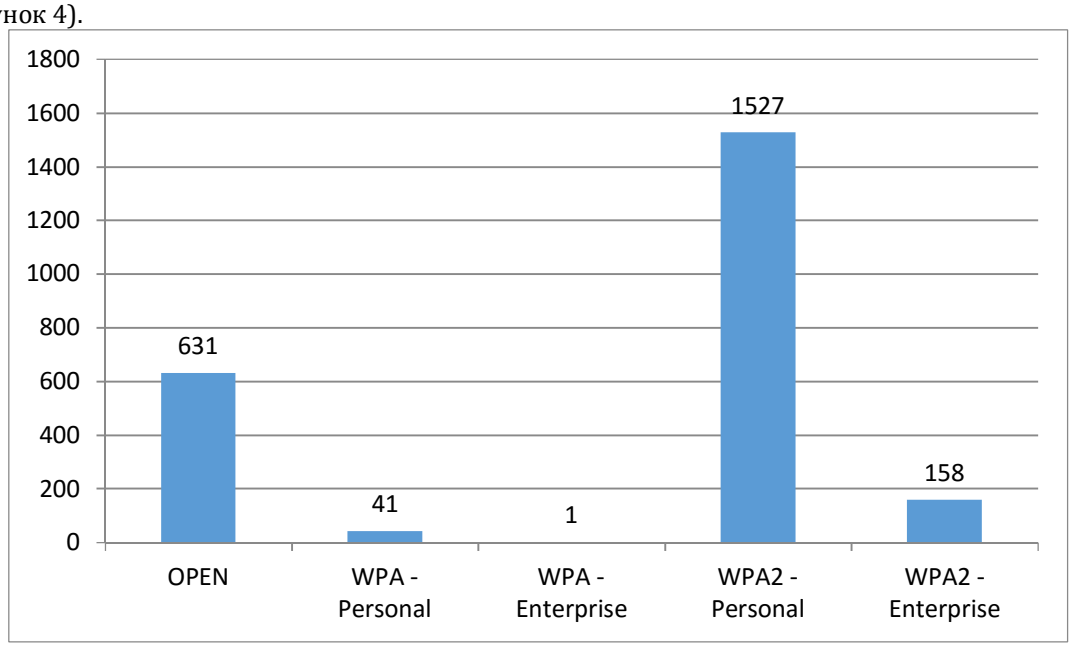

Рисунок 4 – Распределение беспроводных сетей по способу аутентификации

Таким образом, подводя итог, хотелось бы отметить, что проблема безопасности беспроводных сетей на сегодняшний день становится одной из главных проблем IT технологий. Одним из ключевых факторов разработки и проектирования любых системы является безопасность. В защите Wi-Fi-сетей применяются различные алгоритмы математических моделей аутентификации, шифрования данных и контроля целостности их передачи, но, тем не менее, проблема уязвимости сетей остается весьма существенной. Если настройке сети не будет уделено

должного внимания, то злоумышленник будет способен получить доступ к ресурсам пользователей Wi-Fi-сети.

Литература

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2006. – 958с.
2. Постановление Правительства Российской Федерации в связи с принятием Федерального закона "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно – телекоммуникационных статей URL: http://publication.pravo.gov.ru/Document/View/0001201408050024 (дата обращения 14.10.2016)
3. Постановление Правительства Российской Федерации от 12.08.2014 № 801 "О внесении изменений в некоторые акты Правительства Российской Федерации" [электронный ресурс] //
4. URL: http://publication.pravo.gov.ru/Document/View/0001201408190035?index=0&rangeSize=1 (дата обращения 14.10.2016)
5. Таненбаум Э. Архитектура компьютеров. / Э. Таненбаум - СПб.: Питер, 2007. - 848 с.
6. Официальный сайт GlobalSat Technology Corporation — производителя GPS навигационного оборудования различного назначения [электронный ресурс] // URL: http://www.globalsat.ru/catalog/bu-353s4 (дата обращения 14.10.2016).
7. Официальный сайт TP-LINK — производитель компьютерного и телекоммуникационного оборудования.[электронный ресурс] // URL: http://www.tp-linkru.com/products/details/cat-9_Archer-C50.html (дата обращения 14.10.2016).

References

1. Olifer, V. G. Komp'juternye seti. Principy, tehnologii, protokoly / V. G. Olifer, N. A. Olifer. – SPb.: Piter, 2006. – 958 s.
2. Postanovlenie Pravitel'stva Rossijskoj Federacii v svjazi s prinjatiem Federal'nogo zakona "O vnesenii izmenenij v Federal'nyj zakon "Ob informacii, informacionnyh tehnologijah i o zashhite informacii" i otdel'nye zakonodatel'nye akty Rossijskoj Federacii po voprosam uporjadochenija obmena informaciej s ispol'zovaniem informacionno – telekommunikacionnyh statej URL: http://publication.pravo.gov.ru/Document/View/0001201408050024 (date of the application14.10.2016).
3. Postanovlenie Pravitel'stva Rossijskoj Federacii ot 12.08.2014 № 801 "O vnesenii izmenenij v nekotorye akty Pravitel'stva Rossijskoj Federacii" // URL:http://publication.pravo.gov.ru/Document/View/0001201408190035?index=0&rangeSize=1 (date of the application14.10.2016) .
4. Tanenbaum Je. Arhitektura komp'juterov. / Je. Tanenbaum - SPb.: Piter, 2007. - 848 s.
5. Oficial'nyj sajt GlobalSat Technology Corporation — proizvoditelja GPS navigacionnogo oborudovanija razlichnogo naznachenija [jelektronnyj resurs] // URL: http://www.globalsat.ru/catalog/bu-353s4 (date of the application14.10.2016).
6. Oficial'nyj sajt TP-LINK — proizvoditel' komp'juternogo i telekommunikacionnogo oborudovanija.[jelektronnyj resurs] // URL: http://www.tp-linkru.com/products/details/cat-9_Archer-C50.html (date of the application14.10.2016).

Поступила: 15.09.2016

Об авторах:

Аржаков Антон Валерьевич, магистрант кафедры компьютерных систем и технологий Национального Исследовательского Ядерного Университета «МИФИ», zdj22@yandex.ru;

Атавина Анастасия Владиславовна, студент кафедры компьютерных систем и технологий Национального Исследовательского Ядерного Университета «МИФИ», atavina@bk.ru;

Зарешин Сергей Владимирович, магистрант кафедры компьютерных систем и технологий Национального Исследовательского Ядерного Университета «МИФИ», svzareshin@gmail.com;

Сильнов Дмитрий Сергеевич, кандидат технических наук, доцент кафедры компьютерных систем и технологий, Национального Исследовательского Ядерного университета «МИФИ», ds@silnov.pro.