УДК 070.1,004.4
Д. С. Сыч, Е. В. Рафалова, Д. Д. Коваленко, М. А. Сердюкова
г. Гомель, ГГУ имени Ф. Скорины

ИСПОЛЬЗОВАНИЕ ЗАЩИЩЕННЫХ ПОДСЕТЕЙ WI-FI ПРИ ОРГАНИЗАЦИИ РАБОТЫ НАУЧНЫХ КОНФЕРЕНЦИЙ И УЧЕБНЫХ ЗАНЯТИЙ

Незащищенные сегменты сетей WiFi являются атавизмом и признаком плохой организации защиты данных в сетях образовательных учреждений. В таких сетевых сегментах нельзя применять большую часть сетевых сервисов. Одной из основной причин отказа является невозможность организации персонализированного учета услуг и доступность личного трафика пользователя для анализа посторонними лицами либо их оборудованием.

Подключение к сети WiFi предполагает выбор SSID (Service Set Identifier, уникальное имя сегмента беспроводной сети Wi-Fi, которое отображается в списке доступных подключений в программной клиенте операционной системы беспроводной сети). Допустимым сравнением с кабельной инфраструктурой является сопоставление свойств VLAN и SSID (рисунок 1).

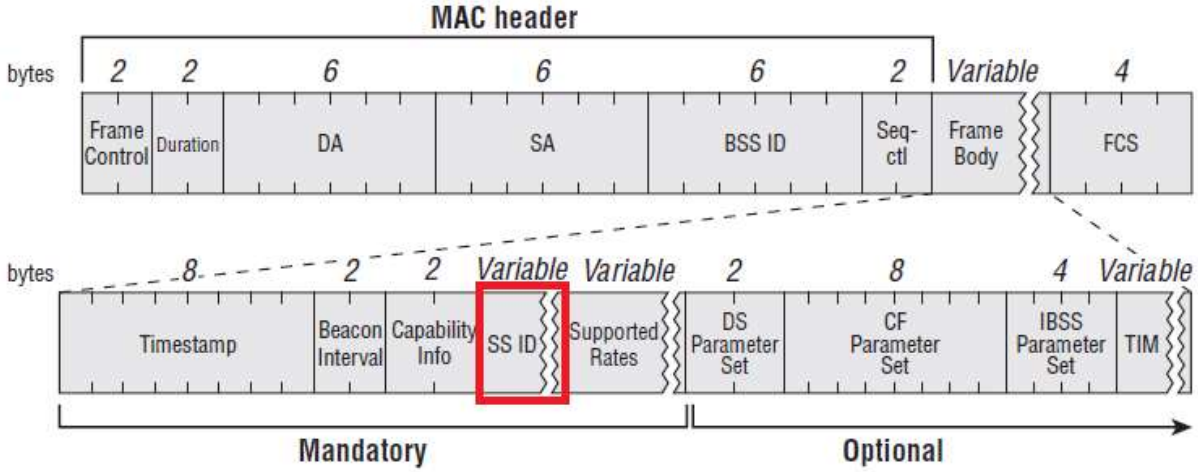

Рисунок 1 – Маркировка сети в формате кадра сети WiFi

Первичная защита сегмента сети WiFi обеспечивается заданием пароля и схемы его шифрования. В современных беспроводных сетях надежной схемой шифрования считается семейство WPA/WPA2/WPA3 [1] .

Регистрация в сегменте сети Wi-Fi с заданным SSID и паролем доступа по QR-коду происходит по быстрому алгоритму: камера смартфона сканирует код, содержащий имя сети (SSID), тип шифрования и пароль, после чего устройство автоматически подключается без ручного ввода данных. Это оптимальный способ поделиться доступом, исключающий публичное разглашение значения пароля. Тем не менее такой подход к защите не является криптостойким.

QR-код создается, например, через онлайн-генератор (https://wifiqrcode.com/).

В этом случае статический QR генерируется для общего использования. Схема получения права доступа к WiFi показана на рисунке 2 [1, 2].

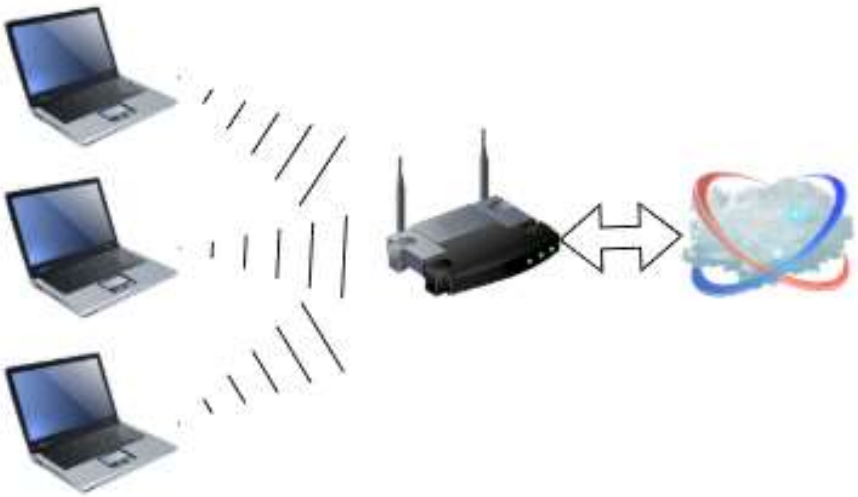

Рисунок 2 – Использование сегмента сети с общим доступом

Общий характер доступа определяет взаимодействие соседних устройств с трафиком участка сети. Полоса пропускания делится между всеми абонентами сети.

После регистрации на устройстве QR передает значение операционной системе, где его можно декодировать штатными инструментами (рисунок 3).

Рисунок 3 – Кодирование и декодирование QR-данных для сети WiFi

Рекомендуется создавать сегмент WiFi с уникальным SSID для каждого события/конференции отдельно и по возможности менять пароль сегмента сети ежедневно.

При организации учебного процесса с регулярным расписанием вышеописанная методика будет вызывать ряд нареканий со стороны пользователей. Для пользователя сети удобно, чтобы он единоразово проходил регистрацию в сегменте сети WiFi и запланированный срок обучения (максимум в течение одного семестра) на одном и том же устройстве не требовалось повторная процедура аутентификации.

В этом случае динамический QR (ваучер) генерируется для индивидуального использования. Схема получения права доступа показана на рисунке 4. Оборудование таких брендов, как MikroTik, Ubiquiti (UniFi), которое применяется в УО «ГГУ имени Ф. Скорины», программно совместимо с этой схемой работы.

Администратор создает ваучеры (вручную или через систему PMS/CRM), указывая срок действия (часы/дни).

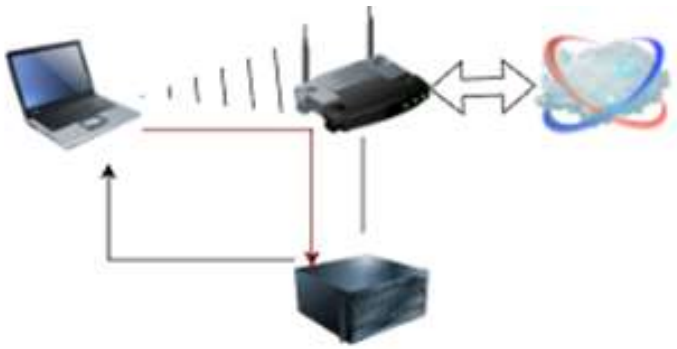

Рисунок 4 – Использование сегмента сети с ваучером

После сканирования QR пользователь попадает на промежуточную страницу авторизации (Captive Portal), где система проверяет валидность токена. На стороне сервера реализован веб-сервис для улучшения юзабилити системы (рисунок 5). Содержимое QR, как правило, не содержит критических данных (SSID, Guest password, IP адрес или URL веб-сервера аутентификации для автоматического перехода на веб-сервис, одноразовая кодовая комбинация), все данные для назначения прав доступа к сети передаются операционной системой клиентского устройства на сторону сервера в рамках защищенного одноразового сеанса связи (MAC адрес устройства, IMEI устройства или цифровой отпечаток операционной системы). При повторном подключении устройства к тому же SSID сети WiFi данные QR уже не являются необходимыми.

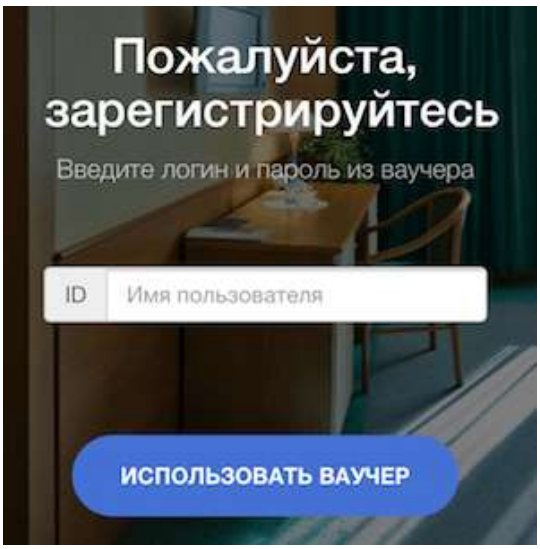

Рисунок 5 – Пример страницы веб-сервиса для активации токена

В случае попытки повторного использования QR для аутентификации с другого устройства доступ для уже зарегистрированного абонента может быть заблокирован, оставлен без изменения и/или ограничен по числу доступных сервисов.

Литература

1. Демиденко, О. М., Кулинченко В. Н., Бычков П. В. Контроль и диагностика внутрипериметральных каналов независимых (смежных) беспроводных сегментов сети / В. Н. Кулинченко, О. М. Демиденко, П. В. Бычков // Известия Гомельского государственного университета имени Ф. Скорины, № 6 (129), 2021. – С. 85–89.

2. Kulinchenko, V. N. Techniques for Passive and Active WiFi Network Surveys // V.N.Kulinchenko, D. L. Kovalenko A. V.Varuyeu, / Материалы X международной конференции «Инжиниринг & Телекоммуникации – En&T 2023». – Moscow – Dolgoprudny : MIPT, 2023. – С. 18–24.