УДК 004.771: 004.056.53 **DOI 10.5281/zenodo.1485604**

Лотюк Ю. Г., к.пед.н., доцент, Соловей Л. Я., ст. викладач, Юскович-Жуковська В. І., к.т.н. доцент (Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука, м. Рівне)

БЕЗПЕКА WI-FI МЕРЕЖІ ОРГАНІЗАЦІЇ

Анотація. *В статті досліджено методи захисту локальної мережі Wi-Fi організації в двох аспектах – захисту від несанкціонованого доступу на фізичному рівні та шифрування переданої інформації. Розглянуто можливість захисту локальної бездротової мережі за допомогою засобів, які вбудовані у програмно-апаратний комплекс мережевих пристроїв. Розкрито небезпеку і вразливість мережі та запропоновано способи захисту. Враховано особливості використання мережі Wi-Fi в разі коли, з одного боку, мають бути доступні деякі специфічні порти, наприклад ssh та ftp, а з іншого, гарантована безпека мережі. Обґрунтовано, що оскільки мережа ззовні, як правило, захищається файрволом організації, найбільшу увагу необхідно приділяти захисту від загроз у середині самої мережі.*
Ключові слова*: захист Wi-Fi мережі, Wi-Fi мережа організації, загрози Wi-Fi мережі, налаштування Wi-Fi роутеру.*

Аннотация. *В статье исследованы методы защиты локальной сети Wi-Fi организации в двух аспектах – защиты от несанкционированного доступа на физическом уровне и шифрования передаваемой информации. Рассмотрено возможность защиты локальной беспроводной сети с помощью средств, встроенных в программно-аппаратный комплекс сетевых устройств. Раскрыты опасность и уязвимость сети и предложены способы защиты. Учтены особенности использования сети Wi-Fi в случае, если с, одной стороны, должны быть доступны некоторые специфические порты, например ssh и ftp, а с другой, гарантирована безопасность сети. Обосновано, что поскольку сеть извне, как правило, защищается файрволом организации, наибольшее внимание необходимо уделять защите от угроз внутри самой сети.*
Ключевые слова*: защита Wi-Fi сети, Wi-Fi сеть организации, Wi-Fi сеть этажа, угрозы Wi-Fi сети, настройка Wi-Fi роутера.*

Annotation*. The methods of protection of the local area network Wi-Fi of an organization in two aspects are considered – protection from unauthorized access on the physical level and encryption of the transmitted information. The protection of the local wireless network with the help of the tools embedded in the hardware and software complex of network devices is considered. The risks and vulnerabilities of the network and the ways of their protection are revealed.*

The features of using Wi-Fi are considered when, on the one hand, certain specific ports, such as ssh and ftp, should be available and, on the other hand, ensure network security. Since the network is protected from the outside of the organization's firewall, the greatest attention is paid to protecting itself from threats inside the network itself. In order to protect it against external invasions, it is proposed to use Huawei's USG6360 firewall, which allows for in-depth analysis of traffic and to recognize most types of applications, network services, to prioritize among various types of traffic, to limit the band for centralized control and terminal management services, users , access rules and security. The popular security protocols are analyzed, for each protocol the stability, efficiency, vulnerability to attacks, etc. is given. The distribution of encryption protocols in relation to network access points is analyzed. Based on this analysis, recommendations for the choice of network equipment are formulated. The theoretical conclusions are illustrated by the example of setting the wireless router RT-N13U to the 802.11n standard, which is part of the Wi-Fi network of the Faculty of Cybernetics of the Academician Stepan Demyanchuk International University. The baseline data for the analysis is the scheme of the room, the characteristics of the access points, the given network parameters. So faculty of cybernetics is located on the fourth floor of one of the educational buildings of IUEH and contains separate lecture rooms, computer classes, departments and offices. The challenge is to provide access to the Wi-Fi network in all these classrooms. An example of this router demonstrates the basic network security settings. Particular attention is paid to adjusting the transmitter power in the RT-N13U router to provide a stable signal only within the premises and not to allow it to go outside the premises.
***Keywords**: Wi-Fi network protection, Wi-Fi network of the organization, threats to Wi-Fi network, Wi-Fi router setup.*

Для використання Wi-Fi частоти 900 МГц, 2,4 ГГц і 5,8 ГГц були відкриті у 1985 р. До цього часу триває розробка стандартів WiFi 802.11, якою займається Institute of Electrical and Electronic Engineers (Інститут інженерів з електротехніки та електроніки) [1]. Стандарт 1-го покоління IEEE 802.11 забезпечував швидкість до 2 Мбіт/с на дальності до 20 м усередині приміщення. Основним недоліком цього стандарту є використання частот 2,4 ГГц, на які впливає побутове та промислове обладнання. Стандарт 802.11b працював на частоті 2,4 Ггц, але швидкість передачі даних скаладала всього 11 Мбіт/с. Це був перший масовий стандарт, який вивів Wi-Fi на світовий ринок. Стандарт 802.11a/g працює в діапазоні 2,4 ГГц, як 802.11b, але при цьому використовує більш швидке OFDM з'єднання стандарту 802.11a, в результаті чого швидкість зросла до 54 Мбіт/с. Сучасний стандарт 802.11n має швидкість до 600 Мбіт/с і дальність всередині приміщень

досягає 70 м. Він використовує антенні системи MIMO, працює на частоті 2,4 ГГц. На його базі було створено стандарт IEEE 802.11ac-2013.

Wi-Fi технологія в наш час є однією з найбільш популярних і зручних для організації бездротової мережі, але в той же час вона несе в собі загрози інформаційній безпеці. Дані, які передаються через таку мережу, можуть бути перехоплені і розшифровані. Це потребує захисту бездротових мереж. Захист може бути організований як за допомогою програмних, так і апаратних рішень. Тому актуальною постає проблема виявлення вразливості мережі та відшукання відповідних засобів її захисту.

Дослідженням безпеки Wi-Fi мереж займається багато інженерів та науковців. Так Л. А. Шувалова [2] пропонує створювати «зону, що охороняється» і фізично не допускати порушника у зону дії Wi-Fi сигналу. Для створення такої зони пропонується підібрати потужність передавача та при необхідності «заекранувати стіни металевою сіткою». Але такі технічні засоби захисту у навчальному закладі організувати складно. Проблему доступу до ресурсів і дисків користувачів Wi-Fi-мережі, а через неї і до ресурсів LAN досліджували О. А. Міщенко, М. М. Радченко, О. Г. Гаврилюк, О. Г. Цатурян [3]. Вони основну увагу приділяють використанню надійних стандартів передачі даних, таких як IEEE 802.11i. При цьому майже не розглядається питання організації у мережі та захисті специфічних ресурсів. Але у бездротовій мережі факультету кібернетики виникає необхідність створення таких ресурсів та організація доступу до них. Компанія SaferVPN [4] пропонує основну увагу приділяти захисту саме мережевого трафіку. Для цього пропонується вхід кожного користувача у мережу здійснювати через VPN підключення. При цьому мало уваги приділяється фізичному захисту Wi-Fi мережі та підбору протоколів передачі. Такий метод підходить для захисту точок доступу загального користування, але не підходить для локальної мережі факультету, коли потрібно оперативно надавати доступ як до локальних так і до глобальних ресурсів.

Метою нашої роботи є дослідження Wi-Fi мережі, як сучасного засобу підвищення ефективності комунікацій. Завданням цього дослідження є аналіз стану організації захисту бездротової мережі на прикладі мережі Міжнародного економіко-гуманітарного університету імені академіка Степана Дем'янчука (МЕГУ) та напрацювання рекомендацій для захисту такої мережі.

Вихідними даними для розрахунку слугували: схема приміщення, характеристика точок доступу, задані параметри мережі. Наприклад, факультет кібернетики розташований на четвертому поверсі одного з навчальних корпусів МЕГУ і містить окремі лекційні аудиторії, комп'ютерні класи, кафедри та кабінети. Задача полягала у забезпеченні доступу до Wi-Fi мережі у всіх цих навчальних аудиторіях.

Безпека Wi-Fi мережі включає в себе два аспекти: це захист від несанкціонованого доступу та шифрування переданої інформації. Для

захисту локальної бездротової мережі в основному користуються засобами, які вбудовані у програмно-апаратний комплекс мережі [5].

Окреслимо основні параметри, за якими визначається безпека Wi-Fi мережі. Одним з найважливіших параметрів, необхідних для отримання доступу, є ідентифікатор мережі SSID. Згідно стандарту 802.11 SSID є ім'я мережі, яке потрібно ввести для входу в мережу. Для захисту мережі потрібно відключити загальну трансляцію ідентифікатора. Це захистить від спроб сторонніх користувачів підключитися до мережі (якщо не будуть задіяні спеціальні засоби сканування).

Для перешкоджання несанкціонованому доступу необхідно закріпити за кожним конкретним користувачем унікальну MAC-адресу. Для подальшої побудови захисту потрібно створювати віртуальні приватні мережі VPN, що забезпечить більш високий рівень захисту та шифрування трафіку.

Для побудови надійного захисту Wi-Fi мережі факультету кібернетики, як одного з структурних підрозділів МЕГУ, необхідно налаштувати протокол безпеки. Протокол WEP із специфікацій стандарту 802.11 – це основний засіб захисту бездротового каналу зв'язку та шифрування трафіку між точкою доступу і комп'ютером. Для встановлення зв'язку з усіма вузлами мережі повинен збігатися секретний ключ довжиною 40 біт (потокове шифрування методом RC4 зі статичним ключем).

Проте на цей час протокол WEP не є достатньо надійним. Так, для отримання секретного ключа достатньо перехопити порядка 7 мільйонів пакетів трафіку бездротової мережі. При середньому завантаженні мережі такий трафік можна зібрати за 5–8 годин і таким чином розшифрувати пароль.

Для більш надійного захисту Wi-Fi у світі був введений новий стандарт безпеки WPA, який є значно стійкішим, порівняно з WEP. У стандарті WPA реалізована динамічна генерація ключів шифрування, що виключає можливість прослуховування трафіку і обчислення статичного ключа, в основу якого покладено протокол TKIP. При передачі даних відбувається перевірка цілісності WEP-пакетів і шифрування кожного WEP-пакета окремим ключем. Кожен пакет в мережі має свій власний унікальний ключ, і додатково до цього кожен пристрій в мережі наділяється ключем, що постійно змінюється через певні проміжки часу [6].

Шифрування пакета здійснюється наступним чином: генерується випадкове число – вектор ініціалізації і WEP-ключ, після чого вони складаються, і отриманим ключем шифрується пакет даних. Подібний підхід дає величезну кількість варіантів ключів, співпадіння ключів хоча б для двох пакетів майже виключене. Поряд з апаратною реалізацією використовується також програмна реалізація цього протоколу. Наприклад, в ноутбуках на базі Intel Centrino можна використовувати WPA при установці Service Pack SP1.

Більш захищеним протоколом є WPA2, з Advanced Encryption Standard (AES) – алгоритмом шифрування, що забезпечує надійний захист і підтримує ключі довжиною 128, 192 і 256 біт. Цей протокол інтегрований в апаратне забезпечення. Так, сертифікат WPA2 отримала мережева карта Intel PRO Wireless 2915ABG. Дослідження розподілу протоколів шифрування відносно мережевих точок доступу виявило, що D-Link є найпопулярнішим в Україні і на цьому обладнанні побудовано більшість централізованих мереж [7]. Захищеність для D-Link по протоколам WEP (43,3%) і WPA (44,9%) приблизно збігається, а також має високий рівень у порівнянні з іншими виробниками (рис. 1).

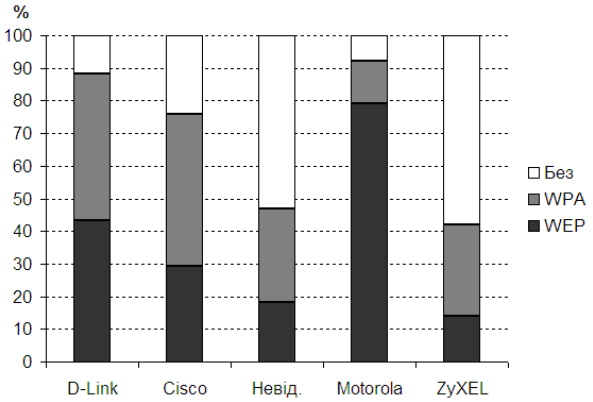

Рис. 1. Використання протоколів шифрування у точках доступу різних виробників

Для гарантування безпеки Wi-Fi мережі і захисту її від зовнішніх вторгнень можна використовувати також міжмережевий екран USG6360 від Huawei, який дозволяє, зокрема, здійснювати поглиблений аналіз трафіку і розпізнавати більшість типів додатків, мережеві сервіси, визначати пріоритет серед різних видів трафіку, обмежувати смугу для сервісів централізованого контролю і управління терміналами, користувачами, правилами доступу і безпекою [8].

Розглянемо налаштування *бездротового маршрутизатора RT-N13U* стандарту 802.11n з інтегрованим принт-сервером. Саме такі маршрутизатори встановлені на факультеті кібернетики Міжнародного економіко-гуманітарного університету імені академіка Степана Дем'янчука [9].

Для налаштування такого бездротового маршрутизатора необхідно встановити протокол передачі даних та алгоритм шифрування (рис. 2).

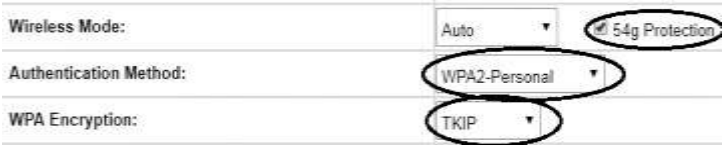

Рис. 2. Встановлення протоколу передачі даних та алгоритм шифрування у маршрутизаторі RT-N13U

Такий крок є обов'язковим, оскільки цим визначається захищеність Wi-Fi мережі. При цьому треба переконатися, що всі клієнтські пристрої підтримують саме ці параметри Ці налаштування унебезпечать роутер від спроб несанкціонованого підключення. Проте, заради бепеки Wi-Fi рекомендується раз на місяць змінювати пароль на підключення. Це обумовлено тим, що при регулярному перехопленні трафіку порушники можуть накопичувати достаню базу і, оримавши доступ до потужних обчислювальних ресурсів, відновити пароль. Доведено, що при систематичному змінюванні пароля шанси порушників зводяться нанівець.

Наступним важливим налаштуванням є налаштування файрвола. (рис. 3).

Рис. 3. Налаштування файрволу у маршрутизаторі RT-N13U

Спочатку його необхідно увімкнути. Наступним кроком є налаштування захисту від DoS атак. Це актуально для роутерів, що безпосередньо включені у мережу Інтернет, а також для роутерів, які мають постійну IP адресу. Відразу доцільно заборонити стороннім особам доступ до роутера через Web інтерфейс, оскільки переважна більшість атак спрямована саме через цей інтерфейс.

Для побутових роутерів основні налаштування можна вважати завершеними. Проте для роутерів, встановлених на факультеті кібернетики МЕГУ, мають бути відкриті порти SSH та FTP. З вікриттям цих портів з'являються додаткові загрози для безпеки. Сервери SSH та FTP мають бути відкриті лише для внутрішньої мережі. Окрім файрвола треба встановити захист від перебору паролів (рис. 4).

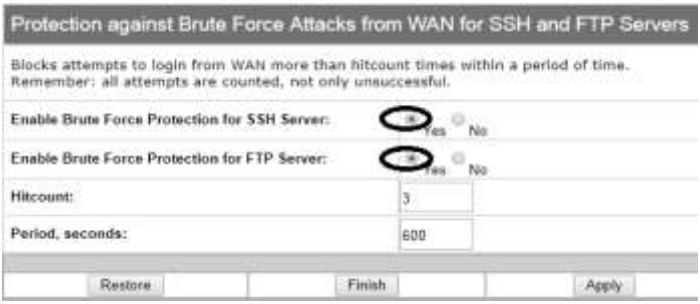

Рис. 4. Встановлення захисту від перебору паролів для SSH FTP з'єднань у маршрутизаторі RT-N13U

Для цього обирають пункти «Enable Brute Force Protection for SSH Server» та «Enable Brute Force Protection for FTP Server». При цьому при «Hitcount» стробах ввести не коректний пароль доступ до відповідного сервісу блокується на «Period, seconds».

Досить важливим є захист від доступу до мережі ззовні приміщення. При розгортанні мережі Wi-Fi у приміщенні потрібно враховувати потужність передавача роутера. Вона програмно регулюється від 1 до 400 mW. Це значення вкажемо у полі «Powerrario» на рис. 5.

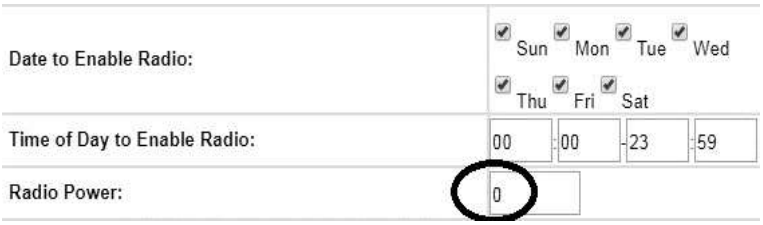

Рис. 5. Налаштування потужності передавача у маршрутизаторі RT-N13U

При цьому потужність має бути такою, щоб забезпечити стійкий сигнал у всіх точках приміщення і унеможливити доступ ззовні. Це детально розглянуто у статті «Моделювання і розгортання Wi-Fi мережі на факультеті кібернетики ПВНЗ «МЕГУ імені академіка Степана Дем'янчука» [9].

З наведеного дослідження можна зробити висновок, що для локальних Wi-Fi мереж основні загрози становлять не стільки технічні засоби проникнення у мережу, як недбалість адміністратора такої мережі. При ігноруванні деяких перерахованих вище налаштувань мережа Wi-Fi залишається повністю працездатною, але вразливою до атак. Вторгнення на

вузол Wi-Fi вдається виявити через деякий час, коли шкода порушниками вже нанесена. Тому потрібно при налаштуванні точки доступу відразу перевіряти всі параметри безпеки, ввімкнути і налаштувати їх, відповідно до стандартів мережевої безпеки.

1. Інститут інженерів з електротехніки та електроніки [Електронний ресурс]. – Режим доступу : https://www.ieee.org/ – Назва з екрану. **2.** Методи захисту даних у Wi-Fi мережах // Наука і техніка Повітряних Сил Збройних Сил України, 2011. – № 2(6). – С. 133–135. **3.** Радченко М. М. Безпека в мережах Wi-Fi. Аналіз основних методів захисту сучасних Wi-Fi мереж / М. М. Радченко, О. А. Міщенко, О. Г. Гаврилюк, О. Г. Цатурян // НЦЗІ ВІТІ ДУТ [Електронний ресурс]. – Режим доступу : http://refua.in.ua/bezpeka-v-merejah-wi-fi.html – Назва з екрану. **4.** Защита при использовании публичных Wi-Fi сетей // SaferVPN [Електронний ресурс]. – Режим доступу : https://www.safervpn.com/ru/what-is-a-vpn/wifi-security – Назва з екрану. **5.** Скопень М. М. Комп'ютерні інформаційні технології: Навч-й пос-к / М. М. Скопень. – К. : Кондор, 2015. – 302 с. **6.** Олифер В. Г. Компьютерные сети: принципы, технологии, протоколы : Учебник для вузов / В. Г. Олифер, Н. А. Олифер. – СПб., 2015. **7.** Исследование защищенности Wi-Fi сетей в г. Киеве – 2008. [Електронний ресурс]. – Режим доступу : https://www.kaa.org.ua/22-articles/57-дослідження-захищеності-wi-fi-мереж-в-м-києві.html – Назва з екрана. **8.** Спортак М. и др. Компьютерные сети и сетевые технологии. Перевод с англ. К. : «ТИД»»ДС», 2012. – 736 с. **9.** Моделювання і розгортання Wi-Fi мережі на факультеті кібернетики ПВНЗ «МЕГУ імені академіка Степана Дем'янчука» // Психолого-педагогічні основи гуманізації навчально-виховного процесу в школі та ВНЗ : Збірник наукових праць. – № 2 (18). – Рівне : РВЦ МЕГУ ім. акад. С. Дем'янчука, 2017. – 292 с. – С. 77–84.

Рецензент: д.ф.-м.н., професор Джунь Й. В.