УДК 004.056

КЛАСИФІКАЦІЯ ЗАГРОЗ ДЛЯ WI-FI МЕРЕЖ

Татарчук Артем, Куперштейн Леонід, Лукічов Віталій

Вінницький національний технічний університет

Анотація

Сьогодні все більше користувачів надають перевагу бездротовим мережам Wi-Fi, що міцно посіли важливе місце в нашому житті. Тому в даній статті запропонована класифікація загроз для бездротових мереж Wi-Fi.

Abstract

Today, more and more users prefer Wi-Fi wireless networks, which have gained an important place in our lives. Therefore, this article presents the classification of threats for wireless Wi-Fi networks.

Вступ

В даний час, в Україні, у зв'язку з входженням у світовий інформаційний простір, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій[1].

Бездротові мережі на сьогоднішній день використовуються практично у всіх сферах діяльності. Широке використання бездротових мереж обумовлено тим, що вони є зручними та мають порівняно невисоку вартість.

Розвиток Wi-Fi технологій спровокує появу нових атак і засобів несанкціонованого отримання інформації. Саме тому актуальним є складання класифікації загроз для бездротових мережі Wi-Fi.

Результат дослідження

Класифікація загроз інформаційної безпеки була створена на основі класифікації запропонованої В. Б. Щербаковим та С. А. Щербаковим [2]. Але запропонована ними класифікація базується на проектуванні архітектури інформаційної безпеки і не може в повній мірі описати множини загроз для бездротової мережі Wi-Fi. Розглянуто класифікацію Панська А.В., Резніченко В.А. [3]. Дана класифікація пропонує тільки мережеві загрози і побудувати повну систему захисту за нею не можливо. Також розглянуто класифікацію Шовкута В. А. та Флорова С. В. [4], ця класифікація розглядає тільки вразливості протоколів безпеки Wi-Fi мереж, які також не підходять для створення системи захисту.

Наведена класифікація може служити етапом в аналізі ризиків інформаційної безпеки Wi-Fi мереж, для аналізу загроз інформаційної безпеки, на її основі можна вибрати методи захисту Wi-Fi мережі.

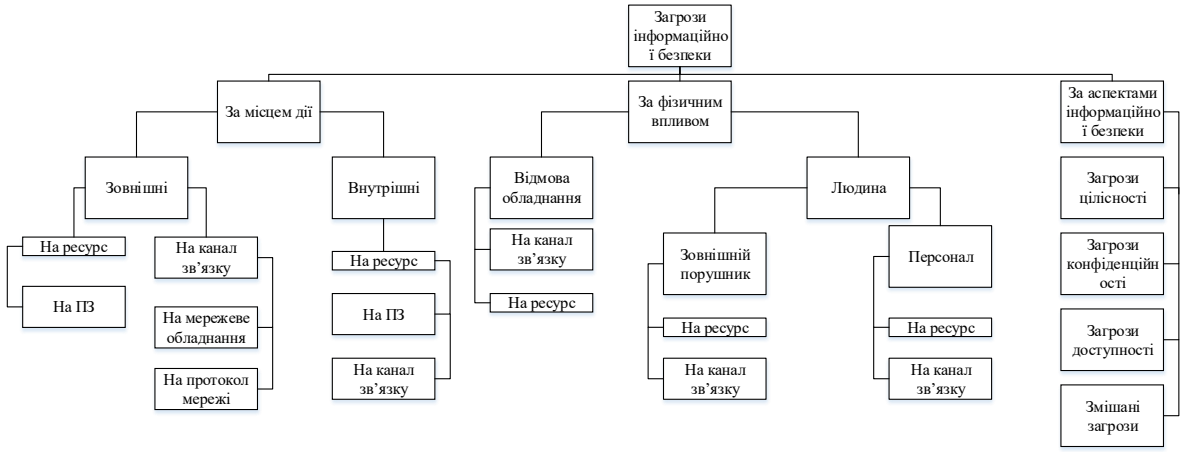
В даній статті наведено класи загроз, за якими можна розподілити конкретні загрози.

Кожен клас загроз має свій вплив: на ресурс, на програмне забезпечення та на канал зв’язку.

Під ресурсом розуміються:

- документація;
- персональні дані;
- інформація, яка знаходиться на базах даних, які пов’язані з Wi-Fi мережею;
- інша інформація, яка потрібна зловмиснику.

До основних загроз можна віднести: Dos-атаки, неправильне налаштування мережі, «випадкові асоціації» (коли ноутбук з Windows XP (досить довірливо ставиться до всіх бездротових мереж) або просто некоректно налаштований бездротовий клієнт автоматично асоціюється і підключає користувача до найближчої бездротової мережі), слабкі ключі шифрування, методи автентифікації з відомими вразливостями,



інтерференції, сканування мережі. Розвиток Wi-Fi мереж породили нові способи реалізації старих загроз, а також деякі нові, досі неможливі в провідних мережах. У всіх випадках, боротися з атакуючим стало набагато важче, тому що неможливо ні відстежити його фізичне місце розташування, ні ізолювати його від мережі. До них відносять: розвідку, імперсонацію, відмову в обслуговуванні.

Практично всі бездротові мережі в якийсь момент з'єднуються з провідними. Відповідно, будь-яка бездротова точка доступу може бути використана як плацдарм для атаки. Але це ще не все: деякі помилки в конфігурації точок доступу в поєднанні з помилками конфігурації провідної мережі можуть відкривати шляхи для витоків інформації. Найбільш поширений приклад - точки доступу, що працюють в режимі моста (Layer 2 Bridge), підключені в плоску мережу (або мережа з порушеннями сегментації VLAN) і передають в ефір широкомовні пакети з дротового сегмента, запити ARP, DHCP, фрейми STP і т.д .

Деякі особливості функціонування бездротових мереж породжують додаткові проблеми, здатні впливати в цілому на їх доступність, продуктивність, безпеку і вартість експлуатації. Для грамотного вирішення цих проблем потрібен спеціальний інструментарій підтримки і експлуатації, спеціальні механізми адміністрування та моніторингу, не реалізовані в традиційному інструментарії управління бездротовими мережами.

Також загрозу мережевій безпеці можуть представляти природні явища і технічні пристрої, проте тільки люди (незадоволені звільнені службовці, хакери, конкуренти) проникають в мережу для навмисного отримання або знищення інформації і саме вони представляють найбільшу загрозу.

Бездротові мережі породжують нові класи ризиків і загроз, від яких неможливо захиститися традиційними засобами. Тому через особливості бездротового зв'язку, важливо контролювати не тільки безпеку інфраструктури доступу, але і стежити за користувачами, які можуть стати об'єктом атаки зловмисника або просто можуть випадково або умисно перейти з корпоративної мережіна незахищене з'єднання.

Список використаних джерел:

1.Концепція технічного захисту інформації в галузі зв'язку України. [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/1126–97–%D0%BF

2.Щербаков В. Б Безопасность беспроводных сетей: стандарт IEEE 802.11. / В. Б. Щербаков, С. А. Ермаков - Москва : РадиоСофт, 2010. - 256 с.

3.Загрози та вразливості бездротових мереж. [Електронний ресурс]. – Режим доступу:http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5022/1/AUConferenceCyberSecurity_November2016_p146.pdf

4.Аналіз механізмів захисту та вразливостей бездротових Wi-Fi мереж. [Електронний ресурс]. – Режим доступу: http://ir.nmu.org.ua/butstream/handle