УДК 004.056

Л. М. Куперштейн
А. Є. Татарчук

ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БЕЗДРОТОВИХ МЕРЕЖАХ WIFI З ВИКОРСТАННЯМ НЕЧІТКОЇ ЛОГІКИ

Вінницький національний технічний університет

Анотація

Розглядається модель оцінки рівня ризику загроз інформаційної безпеки в бездротових мережах WiFi при розрахунку значень ризику за допомогою апарату нечітких множин.

Ключові слова: інформаційна безпека, нечітка логіка, лінгвістична змінна.

Abstract

A model of risk assessment of threats to information security in wireless networks WiFi risk when calculating values using the apparatus of fuzzy sets.

Keywords: information security, fuzzy logic, linguistic variable.

Вступ

Бездротові мережі на сьогоднішній день використовуються практично у всіх сферах діяльності. Широке використання бездротових мереж обумовлено тим, що вони можуть використовуватися не тільки на персональних комп'ютерах, а й телефонах, планшетах і ноутбуках, їх зручністю і порівняно невисокою вартістю.

Однією за найрозповсюдженіших технологій бездротових мереж в бізнесі є WiFi. Її успіх в корпоративних мережах пояснюється простотою розгортання, дешевизною обладнання і відносно високими швидкостями передачі даних в радіоканалі. Разом із тим, такі мережі стають об’єктом атаки зловмисників, дивлячись на певні засоби захисту, передбачені самою технологією.

Розгортаючи мережі WiFi досить часто здійснюється силами здійснюється силами працівників компанії, які не мають відповідної кваліфікації. При чому деякі аспекти захисту можуть бути знехтувані. Це, в свою чергу, може призвести до порушення інформаційної безпеки (ІБ) мережі. Тому на етапах проектування та експлуатації бездротової мережі, доцільним є врахування можливих загроз ІБ та оцінка їх ризиків.

Результати дослідження

До найбільш розповсюджених загроз ІБ мережі WiFi можна віднести: «чужаки», нефіксована природа зв’язку, вразливість мережі та зв’язку, некоректна конфігурація точки доступу, некоректна конфігурація бездротових клієнтів, злам шифрування, відмова в обслуговуванні, підслуховування, особливості функціонування бездротової мережі, витік інформації з мережі [1].

Для оцінки ризиків ІБ поряд із багатьма підходами [2] перевагу віддано апарату нечіткої логіки. Основним компонентом у процедурах нечіткого виведення є база знань нечітких правил, за допомогою якої знання експертів про особливості функціонування деякого об’єкта (системи) подаються у вигляді лінгвістичних висловлювань: якщо <входи>, то <виходи> [3]. Можливість таким чином інтерпретувати експертну інформацію, є безсумнівною перевагою нечіткої логіки

Кількісна оцінка ризику загрози ІБ в мережі зв'язку визначається двома характеристиками - ймовірністю загрози і наслідком від реалізації цієї загрози. На основі моделі з використанням нечіткої логіки визначимо значення ризику загрози «чужаки». Чужаками (RogueDevices, Rogues) називаються пристрої, які дають змогу несанкціонованого доступу до корпоративної мережі, зазвичай в обхід механізмів захисту, визначених політикою безпеки [4]. Заборона на використання пристроїв бездротового зв'язку не захистить від бездротових атак, якщо в мережі, навмисне чи ні, з'явиться чужак. У ролі чужака може виступати все, у чого є інтерфейси: точки доступу (включаючи програмні), сканери, проектори, ноутбуки з обома включеними інтерфейсами і т. д.

Вхідними параметрами є імовірність ризику та збитки від реалізації загроз задані числовими даними. На основі даних параметрів відбувається формулювання терм-множин та лінгвістичних змінних. Лінгвістичні змінні приймають такі значення: імовірність загрози = {Низька ,Середня, Велика}, збиток від реалізації загрози = {Незначний, Низький, Середній, Високий, Неприпустимий}.

Для отримання вихідної змінної ризику загрози ІБ використовуємо алгоритм нечіткого виведення Мамдані [5]. Визначимо лінгвістичні змінні ризику безпеки загрози «чужаки» наступною терм-множиною: низький, помірний, середній, високий, екстремальний.

Етап фазифікації полягає у використанні остаточних правил до вхідних даних (оцінки експертів імовірності і збитку загроз) і служить для конвертації чітких вхідних даних до нечіткого формату. При виборі чисел множин в терм-множні і формулювання функції приналежності терма є суб'єктивною експертною оцінкою. На рис. 1 наведено фрагмент нечіткої бази знань, яка складається з 15 правил.

1. If (Імовірність is Низька) and (Збиток is Незначний) then (Ризики is Дуже_низький) (1)
2. If (Імовірність is Низька) and (Збиток is Низький) then (Ризики is Дуже_низький) (1)
3. If (Імовірність is Низька) and (Збиток is Середній) then (Ризики is Низький) (1)
4. If (Імовірність is Низька) and (Збиток is Високий) then (Ризики is Середній) (1)
5. If (Імовірність is Низька) and (Збиток is Недопустимий) then (Ризики is Високий) (1)

Рис. 1 – Фрагмент нечіткої бази знань продукційних правил

На етапі дефазфікації визначається чітке значення вихідного значення параметру ризику центроїдним методом [5]. Для автоматизації процесу отримання чітких значень ризику ІБ по алгоритму нечіткого виводу Мамдані використано Fuzzy Logic ToolBox системи розробки MATLAB. За отриманими результатами можна розробити рекомендації, щодо побудови системи захисту мережі.

Висновки

Отримані результати можна використати при проведенні аудиту безпеки бездротових мереж, а також для побудови системи підтримки прийняття рішення щодо вибору найбільш безпечної мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Щербаков В. Б Безопасность беспроводных сетей: стандарт IEEE 802.11. / В. Б. Щербаков, С. А. Ермаков - Москва : РадиоСофт, 2010. - 256 с.
2. Астахов А. М. Искусство управления информационными рисками / А. М. Астахов – Москва : ДМК Пресс, 2010. - 312 с.
3. Рутковская Д. Нейронный сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский - Москва : Горячая линия-Телеком, 2006. - 388 с.
4. Шаньгін В. Ф. Захист інформації в комп'ютерних системах і мережах / В. Ф. Шаньгін – Київ : МК Прес, 2012. - 592 с.
5. Корченко А. Г. Построение систем защиты информации на нечетких множествах / А. Г. Корченко - Киев : МК-Пресс, 2006. - 312 с.

Татарчук Артем Євгенович — студент, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, Україна
Куперштейн Леонід Михайлович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет
Tatarchuk Artem — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University
Kupershtein Leonid — PhD, Associate Professor of Information Protection Chair, Vinnytsia National Technical University