

Л. М. Куперштейн, О. П. Войтович, А. Є. Татарчук (Вінниця)

НЕЧІТКИЙ ПІДХІД ДО ОЦІНКИ РИЗИКІВ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ

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 в телефонах, планшетах і ноутбуках, їх зручністю і порівняно невисокою вартістю.

В наш час методи впливу на конкурентів переходять від фізичного впливу до інтелектуального. При цьому використовуються новітні способи і засоби несанкціонованого отримання інформації [1]. Саме тому **актуальним** є необхідність оцінки ризиків інформаційної безпеки для побудови ефективних систем захисту інформації в Wi-Fi мережах.

Постановка задачі. Відомо бездротову локальну мережу з пристроями на основі стандарту IEEE 802.11. Необхідно створити систему оцінки ризиків, яка побудована на застосуванні нечіткої логіки. Системи оцінки ризиків, побудовані на застосуванні нечіткої логіки, можуть характеризуватися логічністю і високою стійкістю в тому випадку, коли аналіз ризиків здійснюється в умовах нестачі даних і знань [2].

Для **розв'язання задачі** запропоновано модель, яка має наступні вхідні параметри: x_1 – імовірність виникнення загрози, x_2 – наявний захист, x_3 – рівень знань порушника, x_4 – рівень можливості порушника, x_5 – рівень збитку підприємства. Вхідні параметри задаються експертом.

Структура моделі має такий вигляд:

$$r = f_r(y, z, x_5);$$

$$y = f_y(x_1, x_2);$$

$$z = f_z(x_3, x_4),$$

де r – рівень ризику, y – імовірність реалізації загрози, z – загальний рівень порушника. Для оцінки значень лінгвістичних змінних $x_1 - x_5$, y , r , z використано шкалу термів: H – низький, HC – нижче середнього, C – середній, BC – вище середнього, E – екстремальний.

За допомогою операції $\min(I)$ отримано систему з 15 рівнянь. Рівняння побудовані на основі експертних знань. Рівняння для змінної r мають наступний вигляд:

$$r_H = (H(y), H(z), H(x_5)) \wedge (C(y), H(z), H(x_5)) \wedge (H(y), C(z), H(x_5));$$

$$r_C = (H(y), C(z), C(x_5)) \wedge (C(y), H(z), C(x_5)) \wedge (C(y), C(z), C(x_5));$$

$$r_{BC} = (C(y), C(z), B(x_5)) \wedge (B(y), C(z), C(x_5)) \wedge (C(y), B(z), C(x_5));$$

$$r_E = (B(y), B(z), C(x_5)) \wedge (B(y), C(z), B(x_5)) \wedge (B(y), B(z), B(x_5));$$

У дослідженні було використано трикутні та трапецевидні функції належності.

Для логічного виведення було використано метод центру ваг [3]. На виході ми отримуємо числове значення від 0 до 100, що означає наскільки мережа несе небезпеку для підприємства. На основі отриманих даних можна зробити висновок, наскільки компанії готова піти на ризик використовуючи дану мережу. За результатом дослідження спроектований програмний додаток.

Висновки. Запропонований підхід до оцінки ризиків інформаційної безпеки в Wi-Fi мережах є досить зручним для формалізації, характеризується логічністю і високою стійкістю, але відсутність достатньої кількості параметрів ускладнює прийняття вірного рішення.

Список літературних джерел

1. Щербаков В. Б. Безопасность беспроводных сетей: стандарт IEEE 802.11. / В. Б. Щербаков, С. А. Ермаков - Москва : РадиоСофт, 2010. - 256 с.
2. Д. Рутковська Нейронні мережі, генетичні алгоритми і нечіткі системи / Д. Рутковська, М. Пилинський, Л. Рутковський. – М: Горячая линия-Телеком, 2006. – 388с.
3. Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, нейронные сети, генетические алгоритмы/ А.П. Ротштейн. - Винница: "Універсум-Вінниця", 1999. - 295 с.