Оцінка Ризиків Інформаційної Безпеки в Мережах Wi-Fi на Основі Апарату Нечіткої Логіки

Леонід Куперштейн
Кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
kupershtein.lm@gmail.com

Олеся Войтович
Кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
voytovych.op@gmail.com

Татарчук Артем
Кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
tatarchuka@bk.ru

Ратников Назар
Кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
nazarratnikov@mail.ru

Information Security Risk Assessment of Wi-Fi Network Based on Fuzzy Logic

Leonid Kupershtein
dept. of Information Protection
Vinnitsia National Technical University
Vinnytsia, Ukraine

Olesya Voytovych
dept. of Information Protection
Vinnitsia National Technical University
Vinnytsia, Ukraine

Tatarchuk Artem
dept. of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine

Ratnikov Nazar
dept. of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine

Анотація—Розглядається модель оцінки рівня ризику загроз інформаційної безпеки в бездротових мережах WiFi за допомогою апарату нечіткої логіки. Використано алгоритм нечіткого виведення Мамдані. Дослідження проведено з використанням інструментарію Fuzzy Logic Toolbox пакету MatLAB.

Abstract—A model of risk assessment of information security threats in WiFi network is considered using fuzzy logic. The algorithm of Mamdani is used. The research was performed using the Fuzzy Logic Toolbox of the MatLAB.

Ключові слова—ризик, інформаційна безпека, загроза, нечітка логіка, лінгвістична змінна.

Keywords—risk, information security, thear, fuzzy logic, linguistic variable.

I. Вступ

Бездротові мережі на сьогоднішній день використовуються практично у дуже багатьох сферах людської діяльності. Широке використання бездротових мереж обумовлено тим, що вони можуть використовуватися не тільки на персональних комп'ютерах, а й телефонах, планшетах, ноутбуках, а а також 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. Саме тому актуальним є необхідність оцінки ризиків інформаційної безпеки для побудови ефективних систем захисту інформації (СЗІ).

Існуючі методи оцінки ризиків в більшості засновані на теоріях ймовірності і класичних множин. Ці методи не дозволяють врахувати той факт, що будь-яка складна система є динамічною системою з набором невизначених даних. 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 [1, 2].

II. Загрози в Wi-Fi мережах

Бездротове середовище передачі радіосигналу створює умови для неконтрольованого підключення до мережі. Класичні способи захисту Wi-Fi мережі, закладені в специфікації її стандартах, включають в себе шифрування і автентифікацію користувачів, і не забезпечують повного захисту мережі. Тому слід визначити ряд загроз, які можна оцінити при побудові чи проведенні аудиту мережі. Загрози Wi-Fi можна поділити на такі групи: «чужаки», нефіксована природа зв'язку, вразливості мереж та пристроїв, нові загрози і атаки, витік інформації з дротової мережі, особливості функціонування бездротових мереж [3 -5].

A. «Чужаки».

Чужаками називаються пристрої, які дають змогу несанкціонованого доступу до корпоративної мережі, часто в обхід механізмів захисту, визначених корпоративною політикою безпеки. Найчастіше це ті самі самовільно встановлені точки доступу. Статистика по всьому світу вказує на чужаків, як на причину більшості зломів мереж організацій. Навіть якщо організація не використовує бездротовий зв'язок і вважає себе захищеною від бездротових атак - впроваджений (навмисне чи ні) чужак з легкістю виправить це положення. Крім точок доступу в ролі чужака можуть виступити домашній роутер з Wi-Fi, програмна точка доступу Soft AP, ноутбук з одночасно включеними дротовим і бездротовим інтерфейсом, сканер, проектор і т.д.

B. Нефіксована природа зв'язку.

Бездротові пристрої не "прив'язані» кабелем до розетки і можуть змінювати точки підключення до мережі прямо в процесі роботи. Наприклад, можуть відбуватися «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. Такий механізм дозволяє зловмисникам «перемикати на себе» нічого не підозрюючого користувача для подальшого сканування вразливостей, фішингу або атак типу «людина в середині».

C. Загрози пов'язані із вразливостями мереж та пристроїв.

Деякі мережеві пристрої, можуть бути більш уразливі, ніж інші - можуть бути неправильно налаштовані, використовувати слабкі ключі шифрування або методи аутентифікації з відомими вразливостями. В першу чергу зловмисники атакують саме їх. Понад 70 відсотків успішних зломів бездротових мереж відбулися саме в результаті неправильної конфігурації точок доступу або клієнтського програмного забезпечення. До вразливостей також відносять злам шифрування, не правильні налаштування клієнтів та точок доступу.

D. Нові загрози і атаки.

Бездротові технології 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.

E. Витік інформації з дротової мережі

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.п . Деякі з цих даних можуть бути корисними для організацій атак Man-in-The-Middle, різних Poisoning і DoS атак, та й просто розвідки.

Інший поширений сценарій ґрунтується на особливостях реалізації протоколів 802.11. У разі, коли на одній точці доступу налаштовані відразу кілька ESSID, широкомовний трафік буде поширяться відразу в усі ESSID. В результаті, якщо на одній точці налаштована захищена мережа і публічний хот-спот, зловмисник, підключений до хот-споту, може, наприклад, порушити роботу протоколів DHCP або ARP в захищеній мережі.

F. Особливості функціонування бездротових мереж.

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

III. Формулювання лінгвістичних змінних

У процесі аналізу факторів ризику виявлено показники, які можуть бути джерелами ризику ІБ в WiFi мережах. При завданні лінгвістичних змінних, що характеризують фактори ризику: ймовірність виникнення загрози - загрози це можливість здійснення загрози по відношенню до будь-якої системи або ресурсу; збиток від загрози це втрати які понесе організація від реалізації загрози; ймовірність реалізації атаки – можливість успішного проведення атаки.

Фактори ризику представлено в формі значення тер-множин:

Ймовірність виникнення загрози (U) = {Низька(Н), середня(С), висока(В)}.

Збиток від загрози (Р) = {Дуже низький(ДН), низький(Н), середній(С), високий(В), дуже високий(ДВ)}.

Ймовірність реалізація загрози (І)= {Низька(Н), середня(С), висока(В)}.

Для отримання вихідної змінної ризику загрози визначимо таку лінгвістичну змінну:

Ризик загрози (R)= {Низький(Н), помірний(П), середній(С), високий(В), екстремальний(Е)}.

IV. Нечітка продукційна модель оцінки ризику

На етапі фазифікації здійснюється встановлення співвідношення між конкретним (чисельним) значенням окремої вхідної змінної системи нечіткого виводу і значенням функції приналежності відповідного їй терму вхідної лінгвістичної змінної. Після завершення цього етапу для всіх вхідних змінних повинні бути визначені конкретні значення функцій приналежності по кожному із лінгвістичних термів, які використовуються в підумовах бази правил системи нечіткого виведення [6, 7].

На рис. 1−3 представлено трикутні функції приналежності лінгвістичних змінних. Трикутні функції приналежності задаються аналітичною формулою:

$$\mu = \begin{Bmatrix} 0, x \le a \\ \dfrac{x-a}{b-a}, a \le x \le b \\ \dfrac{c-x}{c-b}, b \le x \le c \\ 0, c \le x \end{Bmatrix},$$

де [a, c] - діапазон зміни змінної;

b - найбільш можливе значення змінної.

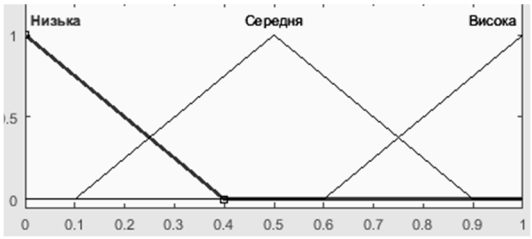

Рис. 1. Функція приналежності ймовірності загрози

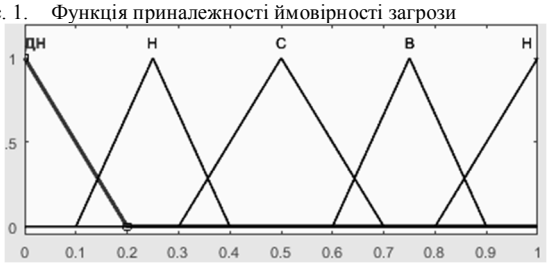

Рис. 2. Функція приналежності збитку від реалізації загрози

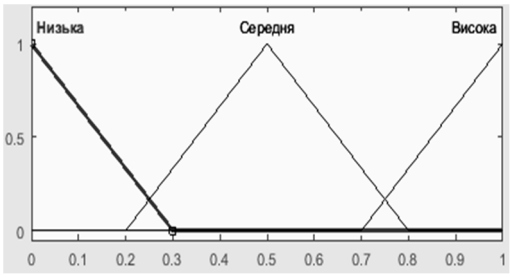

Рис. 3. Функція приналежності ймовірності реалізації загрози

Формування нечітких продукційних правил найчастіше представляється у формі узгоджених щодо використовуваних лінгвістичних змінних структурованого тексту:

ПРАВИЛО_1: ЯКЩО «Умова_1» ТО «Заключення_1» (F 1 т),

...

ПРАВИЛО_n: ЯКЩО «Умова_n» ТО «Заключення_n» (F n т),

де F і ∈ [0; n] є коефіцієнтом визначеності або ваговим коефіцієнтом відповідного правила.

Наприклад:

Правило 1. (U=H and P=ДН and I=H) or (U=C and P=ДН and I=H) or (U=H and P=ДН and I=C) or (U=H and P=H and I =H) or (U=H and P=C and I=H) then R = H.

Правило 2. (U=H and P=C and I=C) or (U=C and P=ДН and I=C) or (U=C and P=H and I=C) or (U=C and P=C and I=H) or (U=B and P=ДН and I=H) or (U=H and P=B and I=H) or (U=H and P=ДН and I=B) or (U=H and P=H and I=B) or (U=H and P=C and I=B) or (U=H and P=B and I=C) or (U=B and P=ДН and I=C) then R = П.

Правило 3. (U=C and P=B and I=H) or (U=C and P=ДН and I=B) or (U=C and P=H and I=B) or (U=B and P=ДН and I=H) or (U=B and P=H and I=H) or (U=B and P=C and I=H) or (U=C and P=C and I=C) or (U=C and P=B and I=C) or (U=B and P=B and I=H) or (U=B and P=ДН and I=C) or (U=C and P=C and I=B) or (U=H and P=B and I=B) or (U=B and P=C and I=H) or (U=B and P=H and I=C) or (U=H and P=C and I=C) or (U=C and P=ДВ and I=C) then R = C.

Правило 4. (U=B and P=C and I=C) or (U=B and P=C and I=B) or (U=B and P=B and I=C) or (U=C and P=B and I=B) or (U=C and P=ДВ and I=B) then R = B.

Правило 5. (U=B and P=B and I=B) or (U=B and P=ДВ and I=B) then R = E.

В алгоритмі Мамдані база правил задається у вигляді структури з трьома входами і одним виходом (рис. 4).

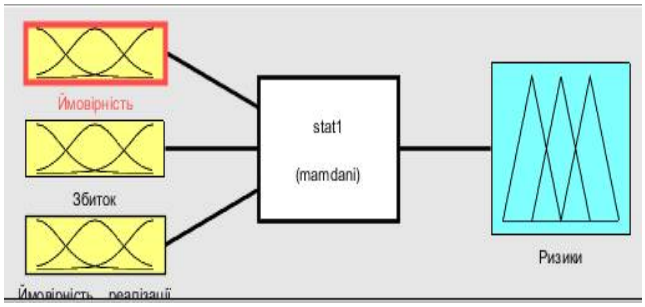

Рис. 4. Структура нечіткої моделі

Етап дефазифікації полягає в тому, щоб, використовуючи результати вихідних лінгвістичних змінних, отримати звичайне кількісне значення кожної із вихідних змінних, яке може бути використано спеціальними пристроями [6].

Перехід від вихідної лінгвістичної змінної до числового значення відбувається методами центру ваги [7]:

$$x = \frac{\int_{\min}^{\max} x\mu(x)dx}{\int_{\min}^{\max} \mu(x)dx},$$

де x − це модальне значення (мода) нечіткої множини, відповідної вихідної змінної після фазифікації.

Реалізуючи систему нечіткого виведення на етапі дефазифікації, отримується оцінка пріоритету ризику. Пріоритезація є основною метою аналізу ризиків і основоположним чинником в процесі прийняття рішень з управління ризиками ІБ організації.

Дослідження було проведено з використанням інструментарію Fuzzy Logic Toolbox пакету MatLAB.

V. Використання моделі оцінки ризиків ІБ Wi-Fi мережі

Припустимо, що на основі попереднього обстеження отримані деякі оцінки рівня захисту мережі, які введемо в вікно механізму виведення графічного інтерфейсу Fuzzy Logic Toolbox.

При значенні ймовірності загрози 0,6, значення лінгвістичної змінної відповідає терму С. При значенні збитку від загрози 0,8 значення лінгвістичної змінної відповідає терму В. При значенні ймовірності реалізації загрози 0,2, значення лінгвістичної змінної відповідає терму Н. За заданими вихідними умовами активізується правило №3. Результуюче значення змінної ризик відповідає значенню 0.5, що визначає значення лінгвістичної змінної С.

На рис. 5 представлено графік «кривої логічного виведення».

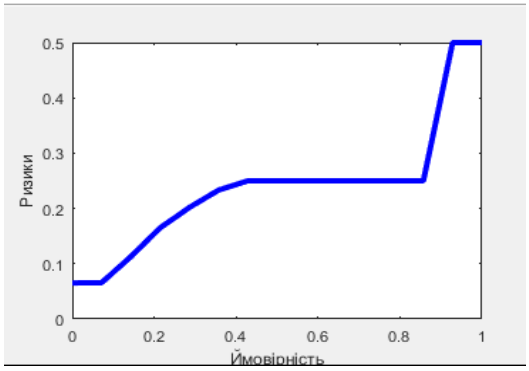

Рис. 5. Залежність змінної R від U

VI. Висновки

Розроблена нечітка продукційна модель оцінки ризиків загроз інформаційної безпеки мереж Wi-Fi дозволяє істотно розширити можливості існуючих методик, зняти обмеження на кількість врахованих вхідних змінних і інтегрувати як якісні, так і кількісні підходи до оцінки ризиків.

Основна складність механізму отримання оцінок ризику на основі нечіткої логіки полягає в побудові моделі для проведення лінгвістичного аналізу ризиків мереж Wi-Fi, однак, даний механізм є ефективним інструментом, коли інші підходи до оцінки ризику неприйнятні. Він володіє широкими можливостями і дозволяє адаптувати його до нових загроз, а також модифікувати з урахуванням реального стану мережі.

Література References

[1] А. Г. Корченко, Построение систем защиты информации на нечетких множествах / А. Г. Корченко - Киев : МК-Пресс, 2006. - 312 с.

[2] А. М. Астахов, Искусство управления информационными рисками / А. М. Астахов – Москва : ДМК Пресс, 2010. - 312 с.

[3] В. Б. Щербаков, Риск-анализ атакуемых беспроводных сетей: Монография/ В.Б. Щербаков, С.А. Ермаков, Н.С. Коленбет; под ред. чл.-корр. РАН Д.А. Новикова. – Воронеж: Издательство «Научная книга», 2013. – 160 с.

[4] В. Б Щербаков, Безопасность беспроводных сетей: стандарт IEEE 802.11. / В. Б. Щербаков, С. А. Ермаков – Москва : Радио Софт, 2010. - 256 с.

[5] В. Ф. Шаньгін, Захист інформації в комп'ютерних системах і мережах / В. Ф. Шаньгін – Київ : МК Прес, 2012. - 592 с.

[6] Д. Рутковская, Нейронный сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский - Москва : Горячая линия-Телеком, 2006. - 388 с.

[7] А.П. Ротштейн, Интеллектуальные технологии идентификации: нечеткие множества, нейронные сети, генетические алгоритмы / А.П. Ротштейн. - Винница: Універсум-Вінниця, 1999. - 295 с.