УДК 004.891.2:004.56:681.5

РОЗРОБКА ЕКСПЕРТНОЇ СИСТЕМИ ДЛЯ ВИРІШЕННЯ ЗАДАЧ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ «РОЗУМНОГО» ДОМУ

В. Г. Крижановський, Д. В. Гончаренко

Безпека та конфіденційність є найбільшими проблемами при розробці рішень для системи «розумного дому». Порушення безпеки системи «розумного дому» може призвести до несанкціонованого доступу зловмисників до особистих даних мешканців, а також доступу до систем керуванням безпекою будинку.

Компанія ESET, яка є лідером в галузі інформаційної безпеки, повідомила про виявлення серйозних уразливостей в безпеці центрів управління системою «розумного» дому [1]. З огляду на отримані висновки, можна констатувати, що розробка нових або покращення наявних систем безпеки для «розумного дому» є актуальним завданням для винахідника.

Ризики, пов'язані з інформаційною безпекою «розумного дому» можна розбити на три фактори: атаки на систему, привабливість скомпрометованої системи та збитки спричинені успішною атакою [2]. Перші два фактори у сукупності дають уявлення про ймовірність порушення безпеки злочинцем, а третій фактор допомагає зважити загальні ризики від втручання. З метою виявлення та запобігання втручання зловмисників у мережу «розумного дому» створено прототип експертної системи.

Експертні системи – це системи, які здатні пропонувати рішення для конкретних проблем в даній області на рівні, який є близьким до рівня експертів у тій же області [3]. Створена нечітка експертна система для захисту інформації у «розумному» домі використовує представлення знань у вигляді лінгвістичних змінних та нечітких правил. Також, застосовуються алгоритми нечіткого виведення для отримання нових знань. Основними компонентами нечіткої експертної системи є інтерфейс фазифікації, база знань, механізм логічного виведення та інтерфейс дефазифікації. Архітектуру нечіткої експертної системи подано на рисунку 1:

Рис. 1

Проектування експертної системи для захисту "розумного" дому складається з наступних етапів: збір даних про кіберзагрози, розробка системи, застосування системи. На першому етапі створюються вхідні та вихідні змінні. У даному випадку вхідними змінними обрано кібертехніки, цілі кіберзлочинців, методи кіберзлочинців. Вихідними змінними є програмне забезпечення, користувачі, обладнання. Дані змінні обрані з огляду на те, що експертна система має аналізувати можливі атаки з боку зловмисників, попереджати та захищати систему «розумного» дому від них. Другий етап полягає у зборі даних про кібер втручання. Оскільки, експертна система моделює знання людини-експерта, системі необхідно передати точні дані про можливі види атак.

До таких атак було віднесено: DoS, доступ до особистих даних, повторні атаки, перехоплення пакетів, перехоплення сеансу користувача, незахищені інтерфейси та шкідливе програмне забезпечення. На наступному етапі створено модель експертної системи. Припускається, що користувач може взаємодіяти з інтерфейсом експертної системи, щоб побачити пораду даної системи про запобігання загрози. Модель експертної системи подана на рисунку 2:

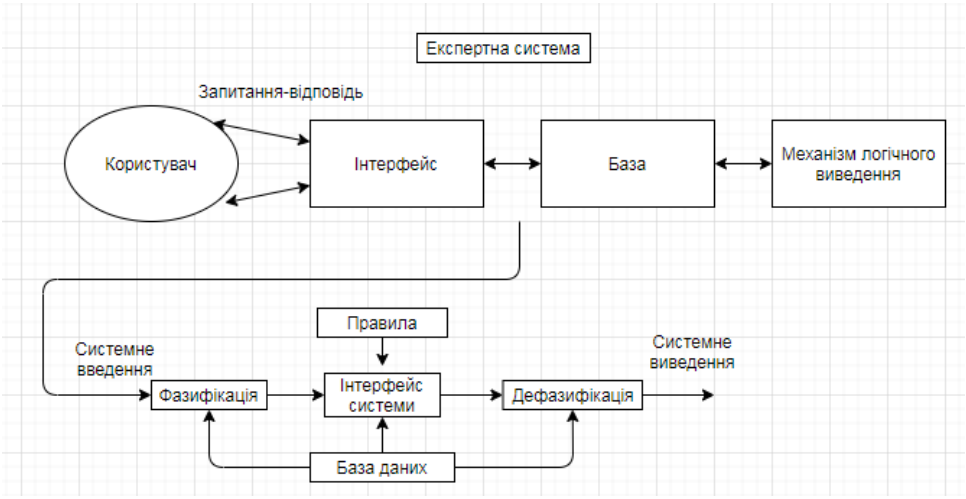

Рис. 2

Основними модулями системи, заснованої на нечітких правилах є фазифікація, нечіткі правила, механізм виведення та дефазифікатор. Модуль фазифікації перетворює вхідні дані в оцінку по нечіткій множині. В даній роботі використано трикутні функції належності. Нечіткі правила складаються з операторів IF – THEN [4]. Нечіткі правила складено у комбінації зі значеннями лінгвістичних змінних. Вхідними та вихідними критеріями моделі є кіберметоди (Cyber methods), цілі зловмисників (Targets of attackers), зловмисники (Malefactors), обладнання (Equipment), програмне забезпечення (Software), мета зловмисника (Goal), користувач (User). Визначено критерії, які описують методи що застосовують зловмисники для кіберзлочину у системі «розумного» дому: мережеві атаки (Network attacks), DoS-атаки (DoS), вірусні атаки (Viral attacks), шкідливе ПЗ (Malware), незахищені інтерфейси (Unprotected interfaces), соціальна інженерія (Social engineering). Критерії намірів кіберзлочинців: відмова роботоздатності системи (System failure), перехоплення веб-інтерфейсу (Web interface interception), контроль сервера (Server control), доступ до особистої інформації (Access to personal information). Залежно від намірів зловмисника, він може використовувати наступні методи: З отриманих критеріїв сформовано деякі правила для експертної системи:

1. $if\ (C\ is\ N)\ and\ (T\ is\ W)\ and\ (A\ is\ A)\ then\ (S\ is\ S)\ (E\ is\ E)$
2. $if\ (C\ is\ DoS)\ and\ (T\ is\ S)\ then\ (E\ is\ TS)$
3. $if\ (C\ is\ Se)\ and\ (T\ is\ Cci)\ and\ (Cit\ is\ Fc)\ then\ (U\ is\ Ut)$
4. $if\ (M\ is\ W)\ and\ (G\ is\ CC)\ and\ (M\ is\ M)\ then\ (S\ is\ SU)$
5. $if\ (M\ is\ Cs)\ and\ (G\ is\ Kl)\ and\ (Ci\ is\ SS)\ then\ (E\ is\ Pc)$

Висновки. Отже, результатом виконаної роботи є виявлення правил для створення експертної системи «розумного» дому. Отримані результати є частковими, оскільки, на даний момент, відображають певну частку від можливих загроз для системи. В подальшому необхідно модифіковувати та додавати нові правила та критерії, оскільки щодня з'являються нові методи та способи доступу зловмисниками до особистої інформації мешканців «розумного» дому. Пріоритетним завданням є розробка автономної експертної системи, яка могла б без взаємодії із користувачем виявляти та знешкоджувати загрози.

Література

1. Milan Fránik, Miloš Čermák. Serious flaws found in multiple smart home hubs: Is your device among them? 2020. URL: https://www.welivesecurity.com/2020/04/22/serious-flaws-smart-home-hubs-is-your-device-among-them/. (дата звернення: 28.04.2021).
2. Tamara Denning, Tadayoshi Kohno. Computer Security and the Modern Home. 2013. URL: https://cacm.acm.org/magazines/2013/1/158768-computer-security-and-the-modern-home/fulltext/. (дата звернення: 28.04.2021).
3. Peter J F Lucas, Linda C Van Der Gaag. Principles of expert systems. - United States: Addison-Wesley Longman Publishing Co., 1991. 412 с.
4. Kozhakhmet K., Bortsova G., Inoue A., Atymtayeva L. Expert System for Security Audit Using Fuzzy Logic: тези доп. наук.-практ. конф., м. Алмати, 2012.