Рисунок 2 – Приклади інтерфейсу мобіільного додатку

Розроблений мобільний додаток дозволяє використовувати запитання закритого типу [4], а також запитання на обрання правильної відповідності та обрання правильної послідовності [5]. Так на рис.2 зображено приклади інтерфейсу робочої програми, де можна побачити екран пройдених тестів (рис 2.а). Екран створених тестів користувачем (рис.2.в).

Список використаної літератури

1. Антонов Ю.С. Комп'ютерні системи тестування на основі технології трирівневих баз даних. *Інформаційні технології і засоби навчання.* 2008. Т.6, №2. URL: https://journal.iitta.gov.ua/index.php/itlt/article/view/133 (дата звертання: 21.04.2021) https://doi.org/10.33407/itlt.v6i2.133
2. 4 самые популярные системы тестирования и оценки персонала. Полный обзор. URL: https://www.ispring.ru/elearning-insights/sistema-testirovaniya (дата звертання: 21.04.2021)
3. Мельничин А., Біляковська О. Система тестування знань на базі інтернет-підходу. Інтернет-Освіта-Наука (ІОН-2014): Матеріали IX міжнародної науково-практичної конференції (14 – 17 жовтня 2014 р.). Вінниця: ВНТУ, 2014. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/5093/248-250.pdf?sequence=1&isAllowed=y (дата звертання: 21.04.2021)
4. Антонов Ю.С., Космінська О.М. Методика аналізу тестових завдань на основі отриманих результатів. *Інформаційні технології і засоби навчання.* 2009. Т.12, №4. URL: https://journal.iitta.gov.ua/index.php/itlt/article/view/81/. (дата звертання: 21.04.2021) https://doi.org/10.33407/itlt.v12i4.81
5. Антонов, Ю. С. (2012). Оцінка повноти відповідей в автоматизованих системах контролю знань. Наукові праці Донецького національного технічного університету, серія Інформатика, кібернетика та обчислювальна техніка, (15), 113-117.
6. Robert C. Martin (Uncle Bob). The Clean Architecture. URL: https://blog.cleancoder.com/uncle-bob/2012/08/13/the-clean-architecture.html

УДК 004.891.2:004.56:681.5

Гончаренко Д.В., *студент 1 курсу СО «Магістр» спеціальності 105 «Прикладна фізика та наноматеріали»*
Крижановський В.Г., *д.т.н., професор, професор кафедри радіофізики та кібербезпеки*

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

Донецький національний університет імені Василя Стуса, м. Вінниця

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:

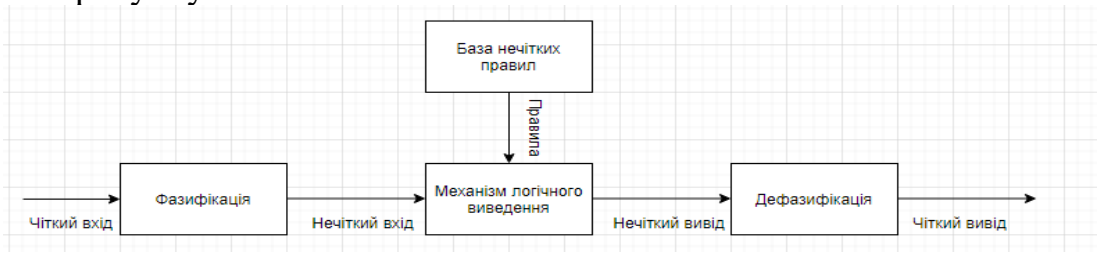

Рисунок 1 – Архітектура експертної системи

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 наступному рисунку:

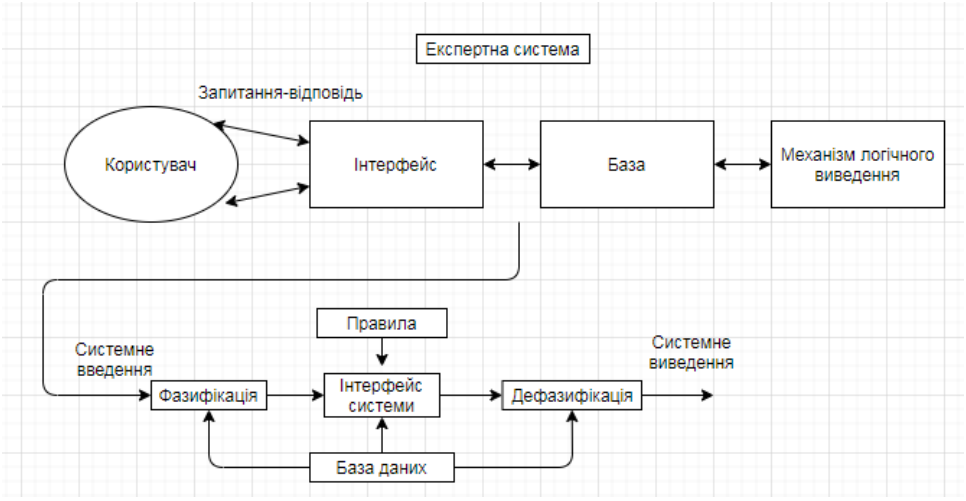

Рисунок 2 – Модель експертної системи

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.

Список використаної літератури:

1. *Fránik M. Serious flaws found in multiple smart home hubs: Is your device among them? [Електронний ресурс] / M. Fránik, M. Čermák. – 2020. – Режим доступу до ресурсу: https://www.welivesecurity.com/2020/04/22/serious-flaws-smart-home-hubs-is-your-device-among-them/.*
2. *Denning T. Computer Security and the Modern Home [Електронний ресурс] / T. Denning, T. Kohno, H. Levy // Communications of the ACM – Режим доступу до ресурсу: https://cacm.acm.org/magazines/2013/1/158768-computer-security-and-the-modern-home/fulltext.*
3. *Peter J. Principles of Expert Systems / J. Peter, L. van der Gaag, L. van der Gaag. – Amsterdam: Addison-Wesle, 1991. – 412 c.*
4. *Kozhakhmet, G. Bortsova, A. Inoue, L. Atymtayeva. Expert System for Security Audit Using Fuzzy Logic, Kazakh-British Technical University, Tole bi st., 59, Almaty, Kazakhstan. MAICS, 2012 (material of conference).*

УДК 004.01

Гораш І.А., *студентка 4 курсу спеціальності «Інформаційна, бібліотечна та архівна справа»*
Січко Т.В., *к.т.н., доцент кафедри комп'ютерних наук та інформаційних технологій*

СИСТЕМНИЙ АНАЛІЗ ОРГАНІЗАЦІЇ (НА ПРИКЛАДІ ДОНЕЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ВАСИЛЯ СТУСА)

Донецький національний університет імені Василя Стуса

Системний аналіз організації – науковий метод, який являє собою послідовність дій з установлення структурних зв'язків між елементами досліджуваної системи, спираючись на комплекс загальнонаукових, експериментальних, природничо-наукових, статистичних, математичних методів [1]. Будь-яка організація, незалежно від її конкретного призначення, може описуватися багатьма параметрами, основними з яких є: визначення цілей організації, структура організації, правова база, особливість функціонування організації, культура організації, характеристика внутрішнього середовища та зовнішнього [2].

Використовуючи системний підхід, розглянемо систему «Донецький національний університет імені Василя Стуса».