to identify vulnerabilities, warn in advance, and improve the response to emergency information [2].

Today Scientists from the University of Barcelona in Spain have developed an algorithm based on artificial intelligence, thanks to which it is possible to combat environmental pollution. The innovative system will be able to detect plastic debris in the ocean directly from the air [3].

Although artificial intelligence offers opportunities to solve environmental problems on our planet, without proper control, the use of artificial intelligence technologies can accelerate the destruction of the environment [4].

With the development of artificial intelligence technologies, it is necessary to assess the possibilities of their direct and indirect applications from an environmental point of view in order to realize their full potential artificial intelligence technologies for the benefit of planet Earth, as well as identify potential risks and develop approaches to minimize them. There are also risks associated with the efficiency and safety of technologies, control over them, the consequences of the use of these technologies [1].

References

1. “Potential Applications of Artificial Intelligence Technologies for the Benefit of the Environment”, available at: https://www.pwc.by/ru/publications/other-publications/ai-research-wef.html (2017)
2. Ben Schiller “How artificial intelligence can help save the planet”, available at: https://rb.ru/story/ai-save-the-planet/»
3. “To save the environment: artificial intelligence taught to identify debris in the ocean from the air”, available at: https://innovation.24tv.ua/ru/iskusstvennyj-intellekt-nauchili-vyjavljat-musor-okeane-vozduha_n1538820 (10 February 2021)
4. “How artificial intelligence can save the planet – research”, available at: https://delo.ua/business/kak-iskusstvennyj-intellekt-mozhet-spasti-planetu-issledovanie-338375/ (25 JANUARY 2018).

Науковий керівник: Краснюк С.О., старший викладач

Stefantsev S., *Senior Lecturer*
Kyiv National Economic University
named after Vadym Hetman
stefancevss@gmail.com

BUILDING A FUZZY COGNITIVE MAP OF THE INFORMATION SECURITY RISK FORMATION MODEL

The conference abstracts deals with the issue of cognitive analysis of conflicts in distributed special-purpose management systems, considers concepts that affect the security of software, builds a fuzzy cognitive map of the model of information security risk formation, quantifies the impact of cognitive modeling conflicts in distributed special-purpose management systems.

Analyzing the data obtained as a result of an expert survey, to build a fuzzy cognitive map of the information security risk formation model, we will use the list of the most common software defects (vulnerabilities and inaccuracies) [1] and identify concepts that affect the security of software: e_1 – External attacks; e_2 – Internal attacks; e_3 – Buffer overflow; e_4 – Errors when working with dynamic memory; e_5 – Software bookmarks; e_6 – Data leaks; violation of the integrity of information resources; e_7 – Compiler-level protection; e_8 – Special tools for protecting system and application resources; e_9 – Obfuscation (entanglement) system; e_{10} – Monitoring the integrity of executable programs based on analyzing their activity and updating them; e_{11} – Quality of software functioning; e_{12} – Information security risks caused by software health problems.

The next step is to determine the strength of the connection that determines the influence of one concept on another and is determined by linguistic terms. The relationships between concepts in a fuzzy cognitive map can be as positive as possible – enhancing the impact of the concept e_i on the concept e_j ($w_{ij} \succ 0$), yes and negative – those that weaken the influence of the concept e_i on the concept e_j ($w_{ij} \prec 0$),that is $w_{ij} \in [-1;1]$.

To solve this problem, we will set a fuzzy linguistic scale: communication strength = {does not affect; very weak; weak; medium; strong; very strong}. Each of these terms corresponds to a numerical range belonging to the segment [0, 1] for positive relations:

$$w_{ij} = \left\{ \begin{array}{l} 0, \text{ does not affect;} \\ (0; 0{,}15], \text{ very weak;} \\ (0{,}15; 0{,}35], \text{ weak;} \\ (0{,}35; 0{,}6], \text{ medium;} \\ (0{,}6; 0{,}85], \text{ strong;} \\ (0{,}85; 1], \text{ very strong.} \end{array} \right\},$$

and a similar numeric range is taken with opposite signs, which belongs to the segment [-1, 0].

Based on the processing of data obtained as a result of an expert survey, we will determine the strength of the relationship between each pair of concepts, which corresponds to a numerical estimate.

The development by experts in the field of Information Technology of a knowledge structure about the information security system, a list of concepts of influence on software security, and the strength of communication between these concepts allows us to build a fuzzy cognitive map of the information security risk formation model (fig. 1).

Modeling was performed using Mental Modeler software tools [2].

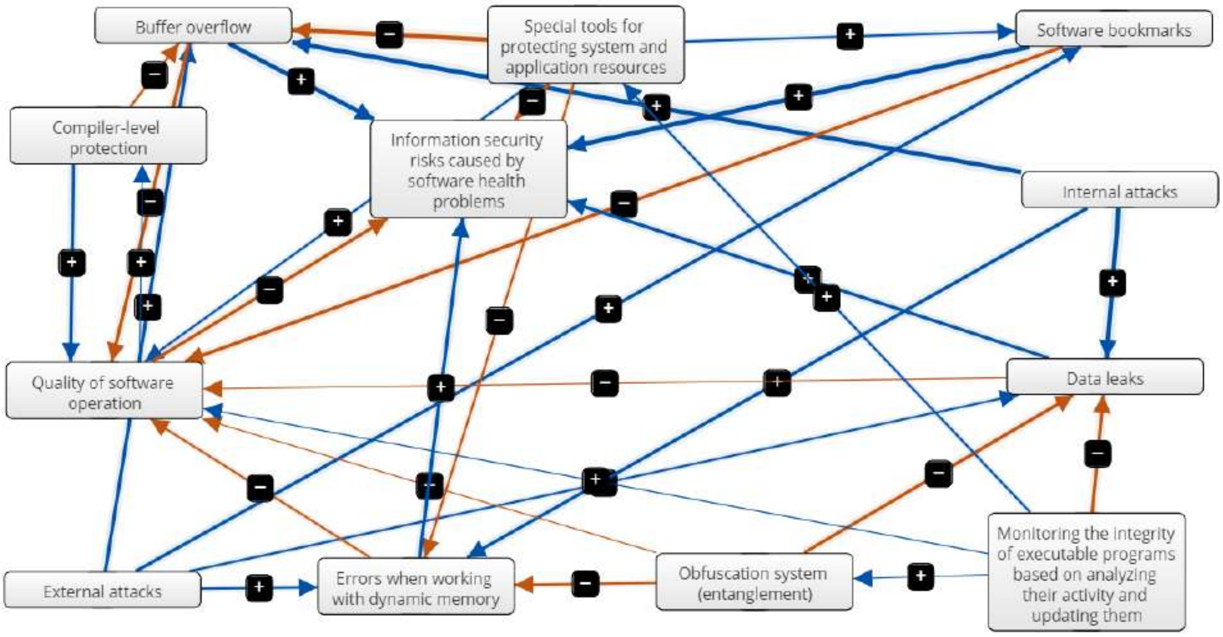
Buffer overflow
Special tools for protecting system and application resources
Software bookmarks
Compiler-level protection
Information security risks caused by software health problems
Internal attacks
Quality of software operation
Data leaks
Monitoring the integrity of executable programs based on analyzing their activity and updating them
External attacks
Errors when working with dynamic memory
Obfuscation system (entanglement)
+
−

Fig. 1. Fuzzy cognitive map of the information security risk formation model

After analyzing the causal relationships between the concepts, we note that the developed fuzzy cognitive map contains: three «Driver» concepts – affect other concepts, but they are not affected by any of the system concepts; one «Receiver» concept – it is influenced by system concepts, but it does not affect any of them; eight concepts of the «Ordinary» type – ordinary, intermediate concepts that are influenced and influenced by certain concepts of the system.

To determine the structural and topological properties of the resulting fuzzy cognitive map, we use the following indicators of the structural complexity of the fuzzy cognitive map:

• fuzzy cognitive map density – shows the degree of connectivity of the graph that displays this fuzzy cognitive map:

$$d = \frac{m}{n(n-1)}, \qquad (1)$$

where m is the total number of connections of the fuzzy cognitive map, and n is the total number of concepts of the fuzzy cognitive map.

In our case, n = 12, m = 31, substituting the corresponding values in Formula (1), we get that d = 0,235. this value indicates a fairly large number of connections between concepts, that is, a high density of the developed fuzzy cognitive map.

• centrality of the concept – characterizes the degree of interaction of the i-th concept of a fuzzy cognitive map with its neighbors:

- initial centrality – shows the total strength of connections (w_{ij}), based on the concept under consideration e_i:

$$od_i = \sum_{j=1}^{n} w_{ij} ; \qquad (2)$$

- input centrality – shows the total strength of connections (w_{ij}),what are included in the analyzed concept e_i:

$$id_i = \sum_{j=1}^{n} w_{ij} ; \qquad (3)$$

- general centrality of the concept:

$$td_i = od_i + id_i . \qquad (4)$$

Calculation of centrality indicators has shown that the concept of e_{12} has the highest structural significance ($td_6 = 4{,}66$),as well as concepts e_3, e_6, e_{11} (indicators td_3, td_6, td_{11} equal respectively 4.45; 3.02; 3.61). These concepts accumulate the greatest number of connections from other concepts, that is, they play the role of peculiar centers of influence in a fuzzy cognitive map in the model of information security risk formation.

• complexity – represents the ratio of the number of concepts of the «Receiver» type to concepts of the «Driver» type. The higher the value of this coefficient, the more complex the maps are since it is assumed that they contain more useful results and fewer controlled impacts on the external environment.

For the developed fuzzy cognitive map of the subject area we, obtain the relation: $\frac{1}{3} \approx 0{,}33$, which indicates insufficiently complex thinking systems.

• hierarchy index (*h*):

$$h = \frac{12 \cdot \sigma_{od}^2}{n^2 - 1}, \qquad (5)$$

where $\sigma_{od}^2 = \frac{\sum_{i=n}^{n} (od_i - \mu_{od})^2}{n}$, $\mu_{od} = \frac{\sum_{i=n}^{n} od_i}{n}$.

For h = 1, the system is completely hierarchical, and for h = 0, it is completely democratic. Democratic systems are more adaptive to changes in the external environment due to their high level of integration and connectivity. In our case, h = 0.2, which indicates a high democratic nature of the system under study.

After analyzing the main indicators of a fuzzy cognitive map of the subject area, we will determine the most influential concepts of the system under study (those concepts that have the greatest value of consonance (outdegree) and influence on the system): Internal attacks; Special tools for protecting system and application resources; External attacks; Buffer overflow.

Conclusions

The model of information security risk formation caused by the implementation of information attacks through characteristic vulnerabilities in the software of a distributed special-purpose management system allows us to solve some applied problems that are characteristic of the correlation of information security events. Despite the enlarged nature of the model and the simplified cognitive display of relationships between concepts, the proposed approach can identify significant relationships between vulnerable and specific software protection mechanisms. The formal presentation of the information security risk formation model in the form of a fuzzy cognitive map allowed us to systematize knowledge of the subject area, statistical data on information security incidents and expert experience in the interests of identifying patterns and quantifying the degree of correlation of heterogeneous vulnerabilities and protection measures to information security risks.

References

1 Avetisyan, A. I., Belevantsev, A. A., Chuklyaev I. I. (2014). The technologies of static and dynamic analyses detecting vulnerabilities of software. Cybersecurity issues, 3(4), 20-28. Retrieved November 08, 2020 from: https://cyberleninka.ru/article/n/tehnologii-staticheskogo-i-dinamicheskogo-analiza-uyazvimostey-programmnogo-obespecheniya.

2 Gray, S. A., S. Gray, J. L. De Kok, A. E. R. Helfgott, B. O'Dwyer, R. Jordan, and A. Nyaki. (2015). Using fuzzy cognitive mapping as a participatory approach to analyze change, preferred states, and perceived resilience of social-ecological systems. Ecology and Society 20(2): 11. Retrieved November 08, 2020 from: http://dx.doi.org/10.5751/ES-07396-200211.

Левченко М.А.*, студент*
ДВНЗ «Київський національний
університет технологій та дизайну»
levnikand@gmail.com

DEEP MACHINE LEARNING

Deep learning is the cutting edge area of machine learning research. It represents several hidden layers of artificial neural networks.

The deep learning methodology applies non-linear transformations and high-level model abstractions on large databases. Recent advances in the implementation of deep learning architecture in numerous areas have already made significant contributions to the development of artificial intelligence.

Recently, machine learning and data mining have come into the spotlight and have become the most popular topics among the research community. Taken together, these areas of study analyze the many possibilities for characterizing databases. Over the years, databases have been collected for statistical purposes. Statistical curves can describe past and present to predict future behaviors. However, over the past decades, only classical methods and algorithms have been used to process this data, while the optimization of these algorithms could form the basis for effective self-learning. Improved decision making can be implemented based on existing values, multiple criteria and advanced statistics methods [1].

Before deep learning was officially established as a new research approach, some applications were implemented as part of the concept of pattern recognition through layer processing. In 2003, an interesting example was developed using particle filtering and Bayesian – belief propagation.