2. Gabryelczyk R., Hernaus T. Business Process Management: Current Applications and the Challenges of Adoption. Cognitione Foundation for Dissemination of Knowledge and Science, 2020.

3. What are NFTs and Why are They Becoming Popular? [Electronic resource]. – Access mode: https://medium.com/tribalscale/what-are-nfts-and-why-are-they-becoming-popularc3ca2c84a4b3

4. Krogstie J. Quality in Business Process Modeling. Springer, 2016.

5. The Best Smart Contract Platforms [Electronic resource]. – Access mode: https://academy.shrimpy.io/post/the-best-smartcontract-platforms

УДК 004.7

МОДЕЛЬ ЗАГРОЗ КІБЕРБЕЗПЕКИ ДЛЯ БЕЗДРОТОВОЇ СИСТЕМИ ОПОВІЩЕННЯ

Божаткін С.М.[1][0000-0002-4653-8880], **Гусєва-Божаткіна В.А.**[2][0000-0002-1117-3391], **к.т.н. Фаріонова Т.А.**[3][0000-0003-3384-4712], **д.т.н. Журавська І.М.**[4][0000-0002-8102-9854], **Пасюк Б.Б.**[5][0000-0002-4634-4090]

E-mail: [1]sergii.bozhatkin@nuos.edu.ua, [2]GusevaBozh@meta.ua, [3]tetyana.farionova@nuos.edu.ua, [4]iryna.zhuravska@chmnu.edu.ua, [5]bwolverine44@gmail.com

CYBER SECURITY MODEL FOR HEALTH-FREE ENVIRONMENT SYSTEMS

Bozhatkin S.M., Guseva-Bozhatkina V.A., Ph.D. Farionova T.A., Dr.Sci. Zhuravska I.M., Pasiuk B.B.

Анотація. В даній роботі сформульовані ключові аспекти моделі загроз кібербезпеки для систем сповіщення за допомогою бездротового мережевого зв' язку.

В ході роботи було проведено аналіз існуючих моделей загроз кібербезпеки, моделі порушника. Визначено, що дані моделі не є такими, які повною мірою описують проблеми кібербезпеки проекту. Тому метою роботи є розробка розширеної моделі загрози кібербезпеки, що побудована за допомогою моделі Cyber Kill Chain.

Ключові слова: оповіщення, публічні мережеві точки доступу, несанкціонований доступ, сервер сповіщень, загрози, кібербезпека, модель загроз кібербезпеки, модель Cyber Kill Chain.

Abstract. This paper set out the key aspects of cyber security threats to models of notification via a wireless network Communications.

In the course of work the analysis of existing models of threats of cybersecurity, model of the violator was carried out. It was determined that these models are not such that fully describe the problems of cyber security project. Therefore, the aim of the work is to develop an extended model of cybersecurity threat, built using the Cyber Kill Chain model.

Keywords: alerts, public wireless access point, unauthorized data access, alert nodes, emergencies, cybersecurity, model of cybersecurity threats, Cyber Kill Chain.

Системи оповіщення служать важливою ланкою в ланцюзі кризової комунікації, вони необхідні для мінімізації втрат при надзвичайної ситуації.

В Україні назріла необхідність заміни існуючих систем оповіщення на автоматизовані, що дозволяють виконувати вимоги, що пред'являються до них в сучасних умовах

Станом на сьогодні відбувається перехід до нових структур організації таких систем з урахуванням сучасного стану технічних засобів зв'язку, захисту від несанкціонованого доступу та розповсюдження шкідливого програмного забезпечення [1,2].

Під час створення систем оповіщення через бездротові точки доступу необхідно враховувати забезпечення захищеності точок доступу від загроза різного роду мережевих атак .

Система безпеки інформаційних систем (в даному випадку, систем оповіщення) базується на моделі загроз та моделі зловмисника [3].

Для створення таких моделей необхідно проаналізувати дані, отримані під час аудиту.

Щоб визначити рівень кібербезпеки бездротової системи оповіщення, пропонується розробити розширену модель загроз на основі моделі «Cyber Kill Chain» та визначити різницю із типовою моделлю загроз [4].

Проведені дослідження дозволяють зробити висновок про використання запропанованої моделі загроз кібербезпеки для бездротової системи оповіщення та оцінити ефективність системи оповіщення з точки зору кібербезпеки.

Література

1. B. Kang, H. Choo, A deep-learning-based emergency alert system, ICT Express, Volume 2, Issue 2, Pages 67-70 (2016). doi: 10.1016/j.icte.2016.05.001.

2. O.Patlaichuk, H.Serbulov (2020). Employees notification systems in the event of emergency situations through public wireless access points. In International Competition of Student Scientific Works: BLACK SEA SCIENCE (Odessa, ONAFT) (pp. 259-270).

3. J. Fruhlinger (2020). Threat modeling explained: A process for anticipating cyber attacks. Retrieved from https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html.

4. What is Cyber-Kill Chain and why it should be taken into account in the defense strategy. https://habr.com/ru/company/panda/blog/327488/.

UDK 004.932.72'1

INCREASING ACCURACY OF THE MEASUREMENT OF PROXIMITY BETWEEN OBJECTS WITH INTERVAL ANALYSIS DURING PATTERN RECOGNITION IN ROBOTIC SYSTEMS

Dr.Sci. Mammadov R.G. [0000-0003-4354-3622],
Mammadov G.M.[0000-0002-2874-6221]
E-mail: rahim1951@mail.ru, qurban_9492@mail.ru

Abstract. When determining the measure of proximity between objects (MPBO) during object recognition, errors arise due to the correlation between the measurements of the parameters of the input and reference objects, the presence of a modular operation in the formulas for evaluating the MPBO, and the presence of a gross error in the measurement results. To eliminate these errors, an algorithm for making decisions based on the results of multiple measurements of the parameters of recognized and reference objects is proposed. According to this algorithm, decisions are made not according to the existing formulas for assessing the MPBO, but by analyzing the intervals for assigning the results of repeated measurements of parameters. recognized and reference objects.

Keywords: pattern recognition, measure of proximity between objects, measurement errors, interval analysis, correlation coefficient, re-measurements