МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ "ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

ПРОБЛЕМИ ІНФОРМАТИКИ ТА МОДЕЛЮВАННЯ (ПІМ-2023)

ТЕЗИ ДВАДЦЯТЬ ТРЕТЬОЇ МІЖНАРОДНОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(*20 – 22 вересня 2023 року*)

Харків

2023

УДК 004.9

Проблеми інформатики та моделювання (ПІМ-2023). Тези двадцять третьої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2023. – 129 с.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ:

- Міністерство освіти і науки України;
- Національна Академія наук України;
- Національний технічний університет "ХПІ", Харків;
- Національний університет "Одеська політехніка", Одеса;
- Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАНУ, Київ;
- Харківський національний університет радіоелектроніки, Харків;
- Донбаська державна машинобудівна академія, Краматорськ;
- Ташкентський інститут інженерів іригації і механізації сільського господарства, Ташкент, Узбекистан;
- Азербайджанський державний університет нафти і промисловості, Баку, Азербайджан;
- Грузинський технічний університет, Тбілісі, Грузія

ISSN 2524-0269

ЖИТТЄВИЙ ЦИКЛ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Член-кореспондент НАН України, д-р техн. наук, проф. В.В. Мохор, канд. техн. наук, ст. дослідник О.О. Бакалинський, ІПМЕ ім. Г.Є. Пухова НАН України, м. Київ; д-р техн. наук, доц. Я.Ю. Дорогий, КПІ ім. Ігоря Сікорського, м. Київ; канд. техн. наук., доц. В.В. Цуркан, КПІ ім. Ігоря Сікорського, ІПМЕ ім. Г.Є. Пухова НАН України, м. Київ

Відповідно до [1], впровадження систем управління інформаційною безпекою у організаціях зводиться до розроблення політик, процедур, настанов. Водночас мета діяльності кожної з них обумовлюється [2], по-перше, діями зацікавлених сторін; по-друге, обробленням інформації. Тож виникає проблема створення якісних технічних рішень збереження властивостей зазначеного активу. Для подолання даної проблеми запропоновано представляти системи управління інформаційною безпекою через їхній життєвий цикл [3, 4].

Життєвим циклом систем управління інформаційною безпекою можливе представлення їхнього змінення від етапу концепції до списання [4]. Насамперед це стосується визначення потреб зацікавлених сторін. Вони використовуються для встановлення вимог до систем управління інформаційною безпекою. Їхнє задоволення досягається створенням альтернативних варіантів архітектур. За обраним варіантом проєктується, аналізується, реалізується та інтегрується відповідне якісне технічне рішення [3, 4]. Дані процеси виокремлено як основу створення адаптованих моделей життєвого циклу систем управління інформаційною безпекою до особливостей діяльності конкретних організацій.

Отже, представлення систем управління інформаційною безпекою через їхній життєвий цикл дозволить як визначати функційні можливості на ранніх стадіях розроблення, так і синтезувати відповідні якісні технічні рішення. Крім того, адаптуватися до особливостей діяльності конкретних організацій з урахуванням потреб зацікавлених сторін від етапу концепції до списання.

Список літератури: 1. ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary. [Valid from 2018-02-07; revised 2023-07-14]. URL: https://www.iso.org/standard/73906.html (accessed on: 25.08.2023). **2.** ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. [Valid from 2022-10-25]. URL: https://www.iso.org/standard/27001 (accessed on: 25.08.2023). **3.** *Мохор В., Цуркан В.* Методологія побудови систем управління інформаційною безпекою. *Захист інформації*. Липень – Вересень 2021. Том 23, № 4. С. 200–211. DOI: http://dx.doi.org/10.18372/2410-7840.23.16766. **4.** ДСТУ ISO/IEC/IEEE 15288:2016. Інженерія систем і програмного забезпечення. Процеси життєвого циклу систем (ISO/IEC/IEEE 15288:2015, IDT). [Чинний від 2018-01-01]. Вид. офіц. Київ : ДП "УкрНДНЦ", 2018. 83 с.