НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ НАН УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА

МАТЕРІАЛИ XXII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ВИПУСК 22

Київ – 2022

Рекомендовано до друку Вченою радою
Інституту проблем реєстрації інформації НАН України
(протокол № 14 від 20 грудня 2022 р.)

Інформаційні технології та безпека. Матеріали XXII Міжнародної науково-практичної конференції ІТБ-2022. – Київ: Інжиніринг. – 132 с. ISBN: 978-966-2344-85-1

До збірника увійшли матеріали доповідей, представлених на XXII Міжнародній науково-практичній конференції «Інформаційні технології та безпека» (ІТБ-2022, 16 листопада 2022 року, м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням функціональної стійкості інформаційних систем, безпеки та живучості критичних інфраструктур, комп'ютерного моделювання складних систем, технологій аналітики даних великих обсягів (Big Data), створення аналітичних систем на основі відкритих джерел інформації (OSINT), моделювання, аналізу та прогнозування процесів мережевої взаємодії, методів і засобів підтримки прийняття рішень.

Для фахівців в області інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.

ISBN 978-966-2344-85-1

ДОКУМЕНТО-ОРІЄНТОВАНИЙ ПІДХІД ДО ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

В. Мохор[1], О. Бакалинський[1], Я. Дорогий[2], В. Цуркан[1, 2]

[1]Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, Київ, Україна
[2]Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
v.mokhor@gmail.com, baov@meta.ua, argusyk@gmail.com, v.v.tsurkan@gmail.com

Розглянуто передумови впровадження систем управління інформаційною безпекою в організаціях. Показано їх визначеність організаційними структурами, політиками, процедурами, настановами. Цим обґрунтовано та сформульовано документо-орієнтований підхід до побудови систем управління інформаційною безпекою.

Keywords: інформаційна безпека, система управління інформаційною безпекою, документо-орієнтований підхід.

Вступ

Системою управління інформаційною безпекою гарантується безпечність діяльності організацій і надання ними послуг завдяки належному оцінюванні ризиків. Відповідно до [1] вона визначається організаційними структурами, політиками, процедурами, настановами та пов'язаними з ними діями стосовно збереження властивостей інформаційних активів. Тож формулювання документо-орієнтованого підходу до побудови систем управління інформаційною безпекою є актуальним завданням [1, 2].

Формулювання документо-орієнтованого підходу

Документо-орієнтований підхід визначається сукупністю способів створення текстових специфікацій і проєктних друкованих та/або електронних документів [1, 3]. Це стосується реалізування вимог до побудови систем управління інформаційною безпекою. Вони

повинні бути доступні як задокументована інформація, наприклад, про сферу застосування, оцінювання, оброблення ризиків [4].

Орієнтованість на документи спонукує до забезпечення їх узгодженості. При цьому побудова систем управління інформаційною безпекою зводиться до оцінювання часу та зусиль для їх створення. Крім того, до відповідності текстовим специфікаціям і проєктним документам [3, 4].

Висновки

Отже, документо-орієнтований підхід до побудови систем управління інформаційною безпекою передбачає встановлення їх відповідності системі документів. Це призводить до складнощів оцінювання повноти, узгодженості та взаємозв'язків між вимогами та проєктом через їх викладення у різних текстових специфікаціях.

Перелік посилань

1. ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary. [Valid from 2018-02-07]. URL: https://www.iso.org/standard/73906.html.
2. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. [Valid from 2013-09-25; revised 2018-12-04]. URL: https://www.iso.org/standard/54534.html.
3. Friedenthal S., Moore A., Steiner R. A Practical Guide to SysML. The Systems Modeling Language. Waltham : Elsevier, 2015. 599 p.
4. ISO/IEC 27003:2017. Information technology. Security techniques. Information security management systems. Guidance. [Valid from 2017-04-12]. URL: https://www.iso.org/standard/ 63417.html.