

АНОТАЦІЯ

Войцеховська Марія Михайлівна. Інформаційна технологія оцінювання рівня культури інформаційної безпеки організації. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки» (12 – «Інформаційні технології»). – Національний університет «Чернігівська політехніка», МОН України, Чернігів, 2020.

В роботі вирішено актуальне *наукове завдання* з розробки моделей та методів інформаційних процесів оцінювання рівня культури інформаційної безпеки організації, які дозволять автоматизувати систему визначення поточного рівня культури інформаційної безпеки організації з врахуванням персональних показників співробітників, актуальних ризиків в галузі інформаційної безпеки та нормативних вимог до ведення безпечної діяльності організації в умовах інформатизації.

Метою дисертаційного дослідження є розробка моделей та методів інформаційної технології комплексного оцінювання рівня культури інформаційної безпеки організації з урахуванням особливостей людино-машинної взаємодії, для підтримки прийняття рішень щодо забезпечення відповідного показника безпеки організації.

Для досягнення поставленої мети були сформульовані такі *завдання дослідження*:

- 1) Сформулювати перелік первинних показників рівня культури інформаційної безпеки організації та її індикаторів.
- 2) Розробити модель інформаційних процесів обчислення рівня культури інформаційної безпеки організації.
- 3) Розробити елементи інформаційної технології визначення рівня культури інформаційної безпеки організації.

- 4) Провести експериментальне дослідження щодо збору та обробки первинної інформації для інформаційної технології оцінювання рівня культури інформаційної безпеки організації.

Об'єкт дослідження – інформаційні процеси визначення культури інформаційної безпеки організації.

Предмет дослідження – методи, моделі та інформаційна технологія комплексної оцінки рівня культури інформаційної безпеки організації з врахуванням особливостей людино-машинної взаємодії.

Основні результати дослідження та наукова новизна роботи полягають в тому, що визначено роль культури інформаційної безпеки у загальній системі інформаційної безпеки організації, враховуючи особливості професійної діяльності та пов'язану з обов'язками взаємодію з інформаційною системою, внутрішнім інформаційним простором та зовнішнім середовищем.

Враховуючи складність формалізації предметної області, було запропоновано скористатися математичним апаратом м'яких обчислень, а саме обчисленнями на основі логіки антонімів, нечіткої логіки та нечіткої кластеризації.

Розроблена модель визначення вимог до рівня культури інформаційної безпеки, яка враховує навички користування технічною складовою системи інформаційної безпеки організації та власне персональні аспекти, що стосуються безпечної поведінки при роботі з інформаційними ресурсами.

Запропонована модель оцінки рівня персональної культури інформаційної безпеки співробітників організації. Оцінювання рівня персональної культури інформаційної безпеки за допомогою ієрархічної системи нечіткого логічного виводу дозволяє сформулювати комплект індивідуальних анкет з врахуванням особливостей професійної діяльності співробітників та їх посадових обов'язків.

Для обрахування загального впливу культури інформаційної безпеки персоналу на рівні безпеки структурного підрозділу та організації

запропонована математична модель, яка враховує особливості професійної діяльності працівників.

На основі аналізу міжнародних стандартів ISO/IEC 27001:2015, ISO/IEC 27032:2016 та наробок з формування культури безпеки на об'єктах критичної інфраструктури запропоновано ієрархічну нечітку модель визначення рівня культури інформаційної безпеки організації, яка дозволяє формалізувати процес обчислення з подальшим наданням рекомендацій щодо вибору заходів, спрямованих на підвищення культури інформаційної безпеки.

Запропонована модель визначення структурних підрозділів, в яких має бути впроваджена культура інформаційної безпеки, а також вибору проектного або процесного підходів для впровадження комплексу заходів для оцінки рівня КІБ, його підвищення та подальшого закріплення в якості корпоративного стандарту.

Вперше розроблена модель інформаційного процесу оцінювання рівня КІБ організації, яка на відміну від існуючих, містить аспекти людино-машинної взаємодії і враховує фактори персональної культури безпеки учасників процесу.

Вперше розроблено метод автоматизованої оцінки рівня КІБ організації, який на відміну від існуючих, базується на використанні нечіткої логіки на основі алгоритму Мамдані, і дозволяє виконувати оцінку поетапно на різних організаційних рівнях.

Дістала подальшого розвитку структура системи ІБ організації за рахунок включення факторів персональної КІБ, що дозволяє враховувати вплив людського чинника на загальну систему безпеки організації.

Дістав подальшого розвитку метод оцінки рівня персональної КІБ на основі компетентнісного підходу за рахунок використання логіки антонімів, що забезпечує підвищення ефективності проведення таких оцінок.

Практичне значення отриманих результатів полягає в тому, що наведені вище наукові результати у своїй сукупності утворюють нову

інформаційну технологію оцінки рівня культури інформаційної безпеки організації. Запропонована інформаційна технологія може бути корисною для керівників ІБ-підрозділів та організацій для підтримки впроваджених систем забезпечення інформаційної безпеки. Розроблені бізнес-процеси та архітектура можуть бути використані як основа для розроблення власних систем моніторингу культури інформаційної безпеки; модель оцінки персональної культури інформаційної безпеки – при призначенні певних рівнів доступу до інформаційних систем; моніторингу поточного рівня культури інформаційної безпеки персоналу, структурного підрозділу та саме організації для визначення прогалів в обізнаності та компетенцій в галузі ІБ; формуванні команд реагування на інциденти, тощо.

Дана інформаційна технологія має наступне практичне втілення.

Модель нечіткого логічного виводу дає можливість проводити оцінку рівня культури інформаційної безпеки без спеціальних навичок, що значно розширює можливості її використання в неспеціалізованих організаціях.

Забезпечення швидкого самооцінювання виконується за допомогою розробленої автоматизованої телефонної системи (чатботу).

Результати дисертаційних досліджень впроваджені:

- при виконанні міжнародного наукового проекту «Cyber Rapid Analysis for Defense Awareness of Real-time Situation – CyRADARS» за грантом NATO SPS, (grant agreement number: G5286), науково-дослідних робіт Національного університету «Чернігівська політехніка» «Моделі та методи оцінювання конвергенції систем компетентностей фахівців з використанням технологій штучного інтелекту» (№0120U101929), «Розробка моделей та методів захисту системи від зовнішніх атак з використанням технологій штучного інтелекту» (№0120U101931) та «Розвиток базового моделюючого комплексу мережі ситуаційних центрів державних органів сектору безпеки і оборони України в інтересах захисту критичної інфраструктури держави та кібербезпеки»

(№0119U000058т) Інституту проблем математичних машин і систем Національної академії наук України;

- на ПАТ «ЧЕЗАРА» під час впровадження тестування персоналу на стадії підбору та приймання на роботу на предмет виявлення базового рівня персональної культури інформаційної безпеки;
- в Державному науково-випробувальному інституті випробувань та сертифікації озброєння та військової техніки при розробці документації інформаційних систем «Інформаційна система з доступом до мережі Internet (ІСД-Internet)» та «Система електронного документообігу (СЕДО)»;
- у навчальному процесі Чернігівського національного технологічного університету (Національного університету «Чернігівська політехніка») при проведенні лекцій та лабораторних робіт з дисципліни «Моделі та системи штучного інтелекту» – в процесі навчання бакалаврів спеціальності 121 – «Інженерія програмного забезпечення» на кафедрі інформаційних технологій та програмної інженерії.

Ключові слова: культура, персонал, організація, обізнаність, інформаційна безпека, організаційна культура, експерт, інформаційна система, інформаційна технологія.