

КОГНІТИВНІ ТА ЗМІШАНІ МЕТОДИ ОЦІНКИ ЗАХИЩЕНОСТІ АВТОМАТИЗОВАНОЇ СИСТЕМИ

Заболотний В.І., Совенко Д.М.

Харківський національний університет радіоелектроніки, Харків, Україна

У роботі розглянуте порівняння методів оцінки захищеності системи при створенні КСЗІ.

Об'єктом дослідження є процес оцінки захищеності автоматизованої системи при створенні комплексної системи захисту інформації.

Предмет дослідження – різновиди методів оцінки захищеності системи.

При створенні на об'єкті інформаційної діяльності комплексу технічно-го захисту інформації треба обстежити інфраструктуру та оцінити захищеність системи. На сьогоднішній день не існує уніфікованого метода цієї оцінки [1].

Когнітивні методи основані на орієнтовних графах. Їхні вершини являють собою концепти, а стрілки показують причинно-наслідкові зв'язки. Кожен такий зв'язок має свій коефіцієнт, що показує вплив одного фактору на інший [2]. Щоб зменшити вплив суб'єктивності думок експертів доцільно використовувати сірі когнітивні карти, які відрізняються використанням інтервальних чисел і в наслідок цього мають більш достовірний результат.

Змішані методи оцінки захищеності використовують як кількісні, так і якісні ознаки. Змішаний метод CRRAMM дозволяє не тільки оцінити захищеність системи, а й виявити контрзаходи щодо них та економічно обґрунтувати необхідність їх вживання [3]. Метод складається з трьох частин, кожна з яких потребує своїх вихідних даних, що ускладнює його.

Порівняння когнітивних та змішаних методів оцінки захищеності дає зрозуміти, що перші з них більш гнучкі і дешеві, а при використанні відповідних когнітивних карт дають гарний результат. Однак, змішані методи є найбільш точними і представлені у вигляді програмних продуктів, що дозволяє автоматизувати процеси оцінки. У той же час вони потребують великої кількості вихідних даних, що вимагає багато часу та ресурсів.

Список літератури

1. Андрухів А.І., Тарасов Д.О. Порівняння Методів Оцінки Захищеності Корпоративних Інформаційних Систем. – 2006. – С. 1.
2. Saliieva O., Yaremchuk Yu. Determining the level of security of the information security system based on cognitive modeling // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 1, pp. 42-49. <https://doi.org/10.18372/2225-5036.26.14669>.
3. Buchik S., Shalayev V. The analysis instrumental methods of identification of risks of information security information and telecommunication systems. <https://doi.org/10.18372/2310-5461.35.11841>.