УДК 004.056.53
Д. Косарик; Р. Козак, к. т. н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАСТОСУВАННЯ МЕТОДУ МОНТЕ-КАРЛО ДЛЯ МОДЕЛЮВАННЯ КІБЕРЗАГРОЗ У МЕДИЧНИХ СИСТЕМАХ

UDC 004.056.53
D. Kosaryk; R. Kozak, PhD., Assoc. Prof.

APPLICATION OF THE MONTE CARLO METHOD FOR MODELING CYBERTHREATS IN MEDICAL SYSTEMS

Кібербезпека медичних інформаційних систем є критично важливою, адже вона забезпечує не лише захист конфіденційних даних пацієнтів, а й безпосередньо впливає на їхнє життя та здоров'я. Актуальність цієї проблеми стала підґрунтям для проведення дослідження, яке охопило аналіз сучасних підходів до управління ризиками, здійснення порівняльного аналізу ризик-орієнтованих моделей, а також виявлення прогалини у методах, які б поєднували оцінку потенційної шкоди для пацієнта з фінансовими наслідками. Запропоновано модель оцінки ризиків кібербезпеки медичних систем із використанням методу Монте-Карло, яка враховує вартість, ефективність та вплив заходів контролю на рівень ризику, дозволяючи ідентифікувати сценарії надмірної чи недостатньої ефективності заходів.

Ключовим об'єктом моделювання у дослідженні є медична інформаційна система, для якої ідентифіковано основні загрози [1] та відповідні засоби захисту [2]. За допомогою симуляційної моделі враховано невизначеність параметрів, таких як шкода пацієнту, ціна та ефективність засобу, і здійснено оптимізацію вибору засобів захисту, дотримуючи балансу між рівнем прийнятного ризику та ресурсами організації [3].

Випробування програмої реалізація моделі показало, що накопичення контролів не завжди підвищує ефективність і може бути економічно необґрунтованим. Ефективність досягається завдяки формуванню взаємодоповнювальних груп заходів, а не їх кількісному збільшенню. Практичне значення моделі полягає у допомозі організаціям приймати обґрунтовані рішення щодо вибору заходів безпеки, забезпечуючи баланс між ризиком та витратами. Вона підвищує обізнаність керівників про реальні ризики, враховуючи не лише фінансові чи репутаційні наслідки, а й вплив на життя пацієнтів.

Дослідження мало деякі обмеження, пов'язані з недостатністю статистичних даних у сфері кібербезпеки медичних систем та необхідністю застосування експертних оцінок для формування ймовірнісних розподілів. Нестача відкритих даних обмежує точність оцінки ймовірностей, тому результати моделювання варто розглядати як орієнтовні та адаптувати під специфіку конкретної організації чи бізнесу.

Розроблена модель може бути застосована для ймовірнісної оцінки ризиків та оптимізації заходів та засобів захисту в медичних інформаційних системах, а також дає змогу сформувати інтегровані стратегії безпеки, що враховують специфіку загроз, пріоритети організації та критичний вплив на пацієнтів.

Література

1. Xu, Yanchen & Tran, Daniel & Tian, Yuan & Alemzadeh, Homa. (2019). Poster Abstract: Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices. 23–24.
2. Almohri, Hussain & Cheng, Long & Yao, Danfeng Daphne & Alemzadeh, Homa. (2017). On Threat Modeling and Mitigation of Medical Cyber-Physical Systems.
3. Aven, Terje & Zio, Enrico. (2013). Foundational Issues in Risk Assessment and Risk Management. Risk analysis : an official publication of the Society for Risk Analysis. 34.