

УДК 004

О. Козленко, О. Кіреєнко

(Фізико-технічний інститут, Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»)

ПРИКЛАД Q-АНАЛІЗУ ДЛЯ СЦЕНАРІЇВ ВИТОКУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

UDC 004

O. Kozlenko, O. Kireenko

AN EXAMPLE OF Q-ANALYSIS FOR INFORMATION LEAKS SCENARIOS IN INFORMATION SYSTEMS

Комп'ютерні та мережеві атаки стали постійною загрозою але методи їх опису часто суперечать один одному. В області інформаційної безпеки ця проблема досить актуальна. Крім того, класифікація та виявлення нападів є складним завданням через сильно збільшену кількість загроз впродовж останніх років. Через це класифікаційні схеми, такі як онтології, є поширеним методом у галузі комп'ютерної та мережевої безпеки.

Q-аналіз елементів та зв'язків дозволяє виявити компоненти, які мають більший вплив на остаточну структуру. Вплив сторони захисту на ці компоненти має більшу вагу так як саме ці елементи мають найбільшу зв'язність з іншими елементами захисту.

Отриманий результат продемонстровано на прикладі системи, вразливої до витоку інформації по трьом напрямам та як вплив окремих елементів дозволяє зменшити розрахунки ризиків.

У цій роботі до вирішення проблеми сценаріїв атак пропонується використання поділу елементів з Verizon Data Breach Report за 2016-2019 роки.

Розроблений метод дозволяє:

- Використовувати Q-аналіз для оцінки елементів системи захисту інформації у інформаційно-комунікаційній системі.
- Визначати обов'язкові/найбільш імовірні пари елементів захисту.
- Знаходити взаємовиключні елементи, що спрощує ідентифікацію сценарію, за яким реалізовувати захист системи.
- Використовувати отриману нечітку онтологію у завданні розрахунку ризиків.

Література.

1. 2016 Data Breach Investigation Report, Verizon Enterprise Solutions, 2015
 2. 2017 Data Breach Investigation Report, Verizon Enterprise Solutions, 2016
 3. 2018 Data Breach Investigation Report, Verizon Enterprise Solutions, 2017
 4. 2019 Data Breach Investigation Report, Verizon Enterprise Solutions, 2018
 5. B.Chandrasekaran, J.R. Josephson, and V.R. Benjamin's, "Ontologies: What are they? Why do we need them?" IEEE Intelligent Systems and Their Applications, vol. 14, pp. 20–26, 1999.
 6. Silvia Calegari and Davide Ciucci, "Integrating Fuzzy Logic in Ontologies," International Conference on Enterprise Information Systems, pp. 66–73, 2006
 7. Aarti Singh, Dimple Juneja and A.K. Sharma, "A Fuzzy Integrated Ontology Model to Manage Uncertainty in Semantic Web: The FIOM", International Journal on Computer Science and Engineering, vol.3, no. 3, pp. 1057–1062, March 2011.
 8. Akinribido, Babajide S. Afolabi, Bernard I. Akhigbe and Ifioke J.Udo, "A Fuzzy-Ontology Based Information Retrieval System for Relevant Feedback" International Journal of Computer Science Issues, vol. 8, issue 1, pp: 382–389, January 2011.
- Obitko M, Snasel V, Smid J. Ontology Design with Formal Concept Analysis. Concept Lattices and their Applications; 2004. p. 111.