Information security risks assessment of information systems using event tree analysis

Vasyl Shutovskyi

Department of physical and technical information protection, National Technical University of Ukraine ”Kyiv Polytechnic Institute”, UKRAINE, Kyiv, Prospect Peremogy, 37, E-mail: v.shutovskyi@gmail.com

The tasks of information security (IS) applied to the information and telecommunication systems (ITS) are in the spotlight at the highest levels of authorities nowadays. Recent examples are the Comprehensive National Cyber-security Initiative of the USA and the public national cyber-security initiative of the UK.

One of the main stages during the process of development and maintenance of the secure systems is the risks assessment.

Among the risks assessment techniques, proposed in the international standard ISO/IEC 31010:2009, the usage of event tree analysis is promising, because of its advantages, such as qualitative risks assessment and visual representation of the information system under consideration and effects of counter-measures applied.

In this research the IS risks assessment for ITS was held. The information and telecommunication system was modeled by a directed graph, which consisted of a hundred vertices. Fuzzy numbers were used as the weighting coefficients of the graph. For the risks assessment the modifications of the following algorithms were used: double-sweep, generalized Floyd’s and Yen’s. They were modified to be applicable for graph with fuzzy weighting coefficients.

The aforementioned algorithms were implemented into the application with graphical user’s interface using integrated development environment QT Creator and programming language C++ with cross-platform widget toolkit QT. The risks assessment of the ITS was carried out using different algorithms. Performance and output of the algorithms for the ITS under consideration were analyzed and conclusions were made.

The future research includes development of the optimization technique of an information security system on the basis of the risks levels assessed by the developed application and the counter-measures data.

Оцінка ризиків інформаційної безпеки ІТС методом аналізу дерева подій

Василь Шутовський

Кафедра фізико-технічних засобів захисту інформації, Національний технічний університет України «Київський політехнічний інститут», УКРАЇНА, м. Київ, пр. Перемоги, 37, E-mail: v.shutovskyi@gmail.com

Запропоновано використання орієнтованого графу з нечіткими вагами для здійснення оцінки ризиків інформаційної безпеки інформаційно-телекомунікаційної системи. На базі алгоритму подвійного спуску, узагальненого алгоритму Флойда та алгоритму Йена розроблено алгоритми для аналізу орієнтованого графу системи. Здійснено порівняльний аналіз цих алгоритмів, а також виконано їх програмну реалізацію.

Ключові слова – інформаційна безпека, технічний захист інформації, аналіз ризиків, оцінка ризиків, інформаційно-телекомунікаційні системи.

I. Вступ

На сьогоднішній день задача по забезпеченню інформаційної безпеки (ІБ) інформаційно-телекомунікаційних систем (ІТС) є надзвичайно актуальною. Високий рівень загроз ІБ для військових та цивільних інформаційних систем призвів до того, що в США вже четвертий рік діє Комплексна національна ініціатива в області комп’ютерної безпеки (“Comprehensive National Cyber-security Initiative”), а у Сполученому Королівстві, в зв`язку зі зростаючими збитками від комп’ютерної злочинності, започатковано національну суспільну ініціативу в області комп’ютерної безпеки [1].

На стадіях життєвого циклу захищених інформаційно-телекомунікаційних систем (при проектуванні, впровадженні та експлуатації) необхідно неодноразово проводити оцінку ризиків ІБ системи. Деталізована оцінка ризиків ІТС дозволяє розробити ефективну систему захисту інформації, контролювати її функціонування та проводити її оптимізацію за різними критеріями.

II. Оцінка ризиків методом аналізу дерева подій

Аналіз методик, наведених у міжнародному стандарті ISO/IEC 31010:2009, показав, що для оцінки ризиків ІБ перспективною є методика, основана на аналізі дерева подій (направленого графу системи). Вона має наступні переваги: графічне представлення послідовності подій з урахуванням хронометражу, взаємозв`язків у підсистемах та «ефекту доміно» [2]. Автори методики передбачаються можливість отримання оцінок ризиків у кількісному вигляді. Представляє інтерес застосування цієї методики для кількісної оцінки ризиків ІБ ІТС, розширюючи її можливості за рахунок використання апарату теорії нечітких множин.

III. Методи аналізу орієнтованого графу

У цій роботі проведена оцінка ризиків ІБ для ІТС, що складалася зі ста компонентів (модель – орієнтований граф, що має сто вузлів). Вагові коефіцієнти ребер графу представлено у вигляді нечітких чисел. Такий підхід дозволяє розширити можливості методики: оперувати кількісними, напівкількісними, якісними вхідними та вихідними даними. Для розрахунку вагових коефіцієнтів було використано нечітку експертну систему [3].

Для обчислення оцінки ризиків було розроблено алгоритми розрахунку найкоротших шляхів, основані на алгоритмі подвійного спуску [4], узагальненому алгоритмі Флойда [4] та алгоритмі Йена [5], які було модифіковано для випадку представлення вагових коефіцієнтів графу у вигляді нечітких чисел.

IV. Програмна реалізація розроблених алгоритмів оцінки ризиків ІБ ІТС

Програмна реалізація розроблених алгоритмів оцінки ризиків була виконана у інтегрованому середовищі розробки QT Creator на мові C++ з використанням крос-платформового інструментарію розробки програмного забезпечення QT.

Одержано ранжовані кількісні оцінки ризиків для розглянутої ІТС при використанні різних алгоритмів (для всіх алгоритму число найкоротших шляхів між кожною парою вершин взято рівним п`ятнадцяти). Час розрахунку ранжованих оцінок ризиків на базі ноутбуку Acer 3810T (процесор – Intel Core 2 Solo 1.4 GHz, оперативна пам'ять – 4 Гб, операційна система – Ubuntu 11.04) для модифікованих алгоритмів становив:

- біля 5 хвилин для узагальненого алгоритму Флойда (розраховувався шлях з кожної вершини в кожну, шлях міг проходити декілька разів через одну й ту ж вершину);
- біля 0.1 хвилини для алгоритму подвійного спуску (розраховувався шлях з заданої вершини в усі інші, шлях міг проходити декілька разів через одну й ту ж вершину);
- біля 1 хвилини для алгоритму Йена (розраховувався шлях з заданої вершини в усі інші, шлях не міг проходити декілька разів через одну й ту ж вершину).

Результати розрахунків по кожному алгоритму є повторюваними.

Результати оцінки ризиків ІБ ІТС, отримані за допомогою модифікованого узагальненого алгоритму Флойда, включають в себе також результати, отримані за допомогою модифікованого алгоритму подвійного спуску. Модифікований алгоритм Йена має найбільший час розрахунку одного шляху, однак розраховані за допомогою цього алгоритму шляхи не містять повторів вершин, що робить цей алгоритм більш зручним при подальших дослідженнях можливості оптимізації системи захисту інформації.

На етапі програмної реалізації алгоритмів оцінки ризиків ІБ ІТС розроблено графічний інтерфейс користувача, який дозволяє отримати візуалізацію графа-моделі системи, що здійснюється на основі силового алгоритму [6], а також результатів оцінювання ризиків ІБ ІТС. Такий підхід дозволяє прискорити роботу з розробленим програмним забезпеченням особі, що приймає рішення.

Висновок

В роботі використання апарату нечітких множин у методі аналізу дерева подій дозволило одержати кількісні оцінки ризиків інформаційної безпеки ІТС.

Проведений порівняльний аналіз роботи модифікованих алгоритмів показав, що алгоритм Йена має найбільший час розрахунку одного шляху, однак розраховані за допомогою цього алгоритму шляхи не містять повторів вершин, в той час як узагальнений алгоритм Флойда працює швидше, але результати менш придатні для подальшої обробки.

Розроблені алгоритми є базовою складовою оптимізації системи технічного захисту інформації ІТС за різними критеріями.

Література

[1] Landwehr C.E. Sailing Away! / Carl E. Landwehr // IEEE Security & Privacy. – The IEEE Computer And Reliability Societies, 2010. – IEEE Security & Privacy, Volume 8, Number 6. – P.3-4.

[2] Risk management — Risk assessment techniques: ISO/IEC 31010:2009. — [Чинний від 01-11-2009]. — Женева: [б.в.], 2009. — 192 с. — (Міжнародні стандарти ISO/IEC).

[3] Шутовський В.О. Розробка адаптивного алгоритму кількісної оцінки ризиків з використанням методів нечіткої логіки / Шутовський В.О. // «Теоретичні і прикладні проблеми фізики, математики та інформатики» Збірка тез доповідей учасників. – 2008. – с. 146.

[4] Майника Э. Алгоритмы оптимизации на сетях и графах: пер. с англ. / Эдвард Майника. — М.: Мир, 1981. — 323 с.

[5] Кристофидес Н. Теория графов. Алгоритмический подход. / Никос Кристофидес. — М.: Мир, 1978. — 432 с.

[6] Brandes U. Drawing on Physical Analogies. / Ulrik Brandes // Drawing graphs: methods and models. – Springer, 2001. – Lecture Notes in Computer Science, Volume 2025. – P.71-86.