ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.056

ВИКОРИСТАННЯ ЕКСПЕРТНИХ ТА НЕЧІТКОЛОГІЧНИХ СИСТЕМ ДЛЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Кущ С.М., к.т.н. доцент, Шутовський В.О., аспірант
Національний технічний університет України
«Київський політехнічний інститут», м. Київ, Україна

Вступ

Побудова комплексних систем захисту інформації (КСЗІ) для інформаційно-телекомунікаційних систем (ІТС) здійснюється на основі оцінювання ризиків інформаційної безпеки (ІБ) ІТС. На даний момент запропоновано ряд методик для проведення оцінки ризиків ІБ ІТС, однак не існує універсальної загально прийнятої методики [1].

Представляє інтерес розробка методики оцінки ризиків ІБ ІТС на основі використання інтелектуальних інформаційних систем [2], до яких відносяться експертні системі (ЕС) та нечіткологічні системи (НС).

Метою роботи є проведення оцінки ризиків ІБ ІТС на основі технологій ЕС та НС.

Оцінювання ризиків ІБ ІТС методом експертних систем

Експертні системи — це інформаційні системи, які містять базу знань, сформовану на основі результатів опитувань експертів у конкретній предметній області [3]. Найбільш ефективним виявилось використання ЕС у вузькоспеціалізованих областях діяльності, для яких сформовані бази даних великих об’ємів. На сьогоднішній день в світі нараховується декілька тисяч експертних систем, що використовуються у різних галузях [4].

В області оцінки ризиків ІБ реалізовано більше десятка програмних комплексів підтримки прийняття рішень, які можна віднести до ЕС. Більшість програмних експертних систем відповідають міжнародному стандарту ISO/IEC 27001:2005 [5]. Деталі методик і алгоритмів, застосованих у цих інструментальних засобах оцінки ризиків ІБ зазвичай є закритими.

Порівняння характеристик найбільш розповсюджених програмних експертних систем, призначених для аналізу ризиків інформаційної безпеки ІТС, наведено в таблиці 1.

Таблиця 1

Властивість \ Експертна система	«COBRA»	«CRAMM»	«Microsoft Security Assessment	«RA2 Art Of	«RiskWatch»	«АванГард» («РискМенеджер»)	«Гриф»
Базовий варіант оцінки ризиків ІБ	+	+	+	+	+	-	-
Повний варіант оцінки ризиків ІБ	-	+	-	+	-	+	
Відповідність стандартам ISO 2700x	-	+	+/-	+	+	+	+

Серед ЕС, які використовуються в області ІБ, однією з найбільш деталізованих є система CRAMM. Процес оцінки ризиків ІБ ІТС з використанням цієї системи складається з наступних етапів [6]:

• підготовчого (збирається загальна інформація про організацію та складається план проведення опитувань);

• ідентифікації та оцінки активів (здійснюється моделювання та оцінювання активів, враховуючи три властивості інформації: конфіденційність, цілісність, доступність – оцінка кожної властивості активу здійснюється окремо за десятибальною шкалою);

• ідентифікації та оцінки загроз та вразливостей (оцінки загроз проводяться за п’ятибальною шкалою, а вразливостей за трьохбальною);

• аналізу ризиків (на основі одержаних на попередніх етапах результатів за семибальною шкалою).

Також представляє інтерес експертна система «Microsoft Security Assessment Tool» (MSAT) [7], яка дозволяє отримати якісну оцінку ризиків ІБ за чотирма характеристиками ІТС: інфраструктура, програмне забезпечення, функціонування, персонал. Для кожної з цих характеристик доступні якісні оцінки ризиків ІБ. Оцінки ризиків ІБ ІТС проводиться за трьохбальною шкалою.

Процес оцінки ризиків ІБ з використанням ЕС MSAT заключається у заповнені полів бази даних експертної системи. На основі цього ЕС формує звіт з переліком якісних оцінок ризиків ІБ ІТС та пропозицій стосовно покращення організації КСЗІ.

Експертні системи CRAMM і MSAT представляють різні класи ЕС. CRAMM дозволяє отримати детальну оцінку ризиків ІБ і містить великий перелік загроз, наслідків та контрзаходів, в той час як MSAT є інструментом для швидкого проведення оцінювання ризиків ІБ ІТС та визначення основних слабких та сильних місць КСЗІ. Використання експертних систем дозволяє автоматизувати процес оцінювання ризиків ІБ, формувати

анкети та звіти, на основі оцінок окремих активів отримати інтегральну оцінку ризиків ІБ ІТС.

Перевагами розглянутих ЕС є уніфікація та автоматизація процесу оцінювання ризиків ІБ на основі наявних стандартних баз загроз, вразливостей, активів. Основними недоліками ЕС як класу систем є те, що аналіз може бути проведений, в основному, для статичних моделей.

ЕС CRAMM дозволяє проводити обробку результатів анкетувань персоналу організації, в неї закладено широкий набір типових рекомендацій по проведенню контрзаходів для зменшення ризиків ІБ ІТС, але її ефективне використання можливе тільки сертифікованими спеціалістами високої кваліфікації. Використання MSAT не вимагає високої кваліфікації спеціаліста та дозволяє швидко провести оцінювання ризиків ІБ ІТС, однак отримані результати мають якісний характер.

Представляє інтерес використання нечіткологічних систем для оцінки ризиків ІБ ІТС, що дозволяє одержати кількісні результати, оперувати вхідними даними різної розмірності (у тому числі безрозмірними) і не потребує високої кваліфікації при експлуатації.

Оцінювання ризиків ІБ методами нечіткої логіки

Системи, що використовують нечітку логіку (нечіткі системи, системи управління на основі нечіткої логіки, нечіткі експертні системи, нечіткологічні системи), отримали широке застосування у системах управління та підтримки прийняття рішень.

В області оцінки ризиків ІБ запропоновано ряд реалізацій нечітких експертних систем, ядром яких є системи нечіткого логічного виводу (СНЛВ, рис.1) [8] та систем, в яких оцінювання ризиків ІБ виконується на основі

Рис.1. Система нечіткого логічного виводу [7]

методів аналізу сценаріїв, модифікованих для використання нечітких чисел в якості вхідних та вихідних даних.

Процес оцінювання ризиків ІБ з використанням СНЛВ включає наступні етапи:

- моделювання загроз ІТС;
- оцінювання ймовірностей реалізації загроз та збитків від їх реалізації;
- формування нечіткої бази знань та функцій належності нечітких змінних у відповідності до профілю ІТС і моделі загроз;
- розрахунку оцінок ризиків ІБ для окремих загроз (на основі СНЛВ) та інтегральної оцінки ризику ІБ ІТС.

Використання системи нечіткого логічного виводу дозволяє розширити можливості існуючих ЕС. Вхідні величини (ймовірність реалізації загрози та збитки від її реалізації) можуть оброблятися СНЛВ як у чіткому, так і у нечіткому вигляді, розраховуватися на основі експертних оцінок, статистичними або іншими методами.

До переваг систем, що використовують нечітку логіку, слід віднести здатність систем оперувати нечіткими вхідними змінними, включаючи динамічні параметри, наборами числових даних (експертними оцінками, статистичними даними і т.д.); можливість оцінювання якості вхідної інформації і надійності джерела інформації, ступеня довіри до нього; настройки параметрів відповідно до різноманітних профілів прикладних систем; проведення аналізу моделей складних динамічних систем; отримання кількісних результатів. Але такий підхід характеризується складністю оцінки вхідних параметрів для системи оцінки ризиків ІБ та формуванням функцій належності й бази знань, адекватних профілю прикладної системи, для якої проводиться оцінка ризиків ІБ.

Застосування теорії нечіткої логіки дозволяє розширити можливості ЕС, тому представляє інтерес порівняння результатів оцінки ризиків ІБ, отриманих з використанням ЕС та НС.

Оцінка ризиків ІБ тестової ІТС методами ЕС та СНЛВ

В роботі проведено оцінювання ризиків ІБ для тестової ІТС (рис.2), використовуючи експертні систем CRAMM та MSAT, а також нечітку експертну систему на основі СНЛВ. Для ІТС сформовано модель загроз на основі переліку загроз додатку F «CRAMM User Guide» [6].

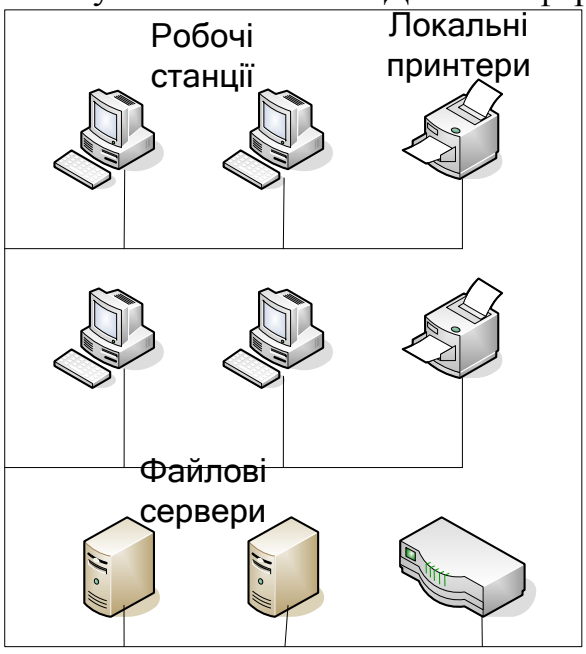

Рис.2. Тестова ІТС [6]

Розрахунки оцінок ризиків ІБ з використанням СНЛВ проводились для випадку, коли база знань формувалась на основі даних, приведених у «CRAMM User Guide» [6] та національному стандарті США NIST 800-30 [9]. Настройка баз знань та функцій належності також проводилась методами параметричної оптимізації та еволюційного програмування [10].

ЕС MSAT не призначена для детального аналізу ризиків ІБ ІТС. Її використання дозволяє отримати тільки якісні оцінки стану захищеності компонентів КСЗІ, і тому порів-

няння з результатами, отриманими при використанні CRAMM та СНЛВ, не представляється доцільним. Фрагмент вікна програмного забезпечення (ПЗ) ЕС MSAT з результатами оцінювання ризиків ІБ ІТС наведено на рис.3.

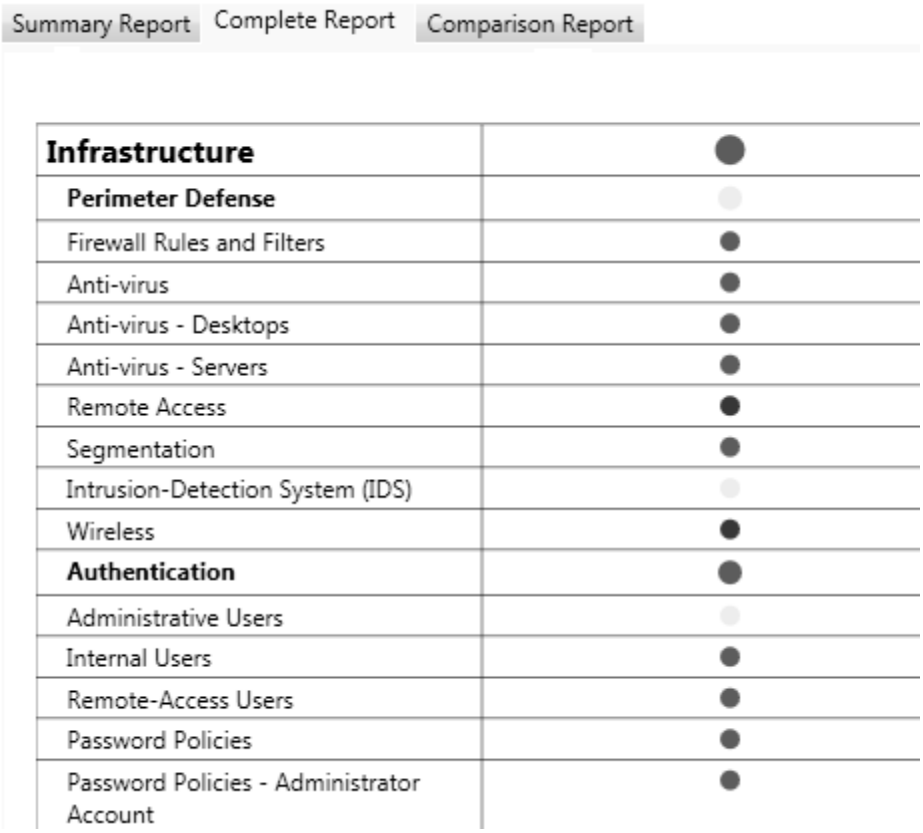

Рис.3. Результати оцінювання ризиків ІБ ІТС для ЕС MSAT

Результати оцінювання ризиків ІБ ІТС для CRAMM та СНЛВ наведено у таблиці 2.

Таблиця 2

№	Назва загрози	Оцінка ризику ІБ (семибальна шкала)	
		CRAMM	СНЛВ
1	Внесення в систему шкідливого ПЗ (introduction of damaging or disruptive software)	1	1
2	Зловживання ресурсами системи (misuse of system resources)	1	1
3	Збій систем зв`язку (communication failure)	3	2
4	Технічний збій ПК (technical failure of host)	1	2
5	Технічний збій мережевого інтерфейса (technical failure of network interface)	1	1
6	Збій прикладного ПЗ (application software failure)	3	2
7	Помилки при обслуговуванні обладнання (hardware maintenance error)	2	2

В результаті аналізу оцінок ризиків ІБ типової ІТС, отриманих при використанні НС та ЕС CRAMM, показано, що результати відносяться до одного кластеру.

Як показав досвід експлуатації, СНЛВ є простішою в застосуванні, а настройка параметрів СНЛВ методами еволюційного програмування та параметричної оптимізації дозволяє застосовувати цю систему для різних класів ІТС [10].

Висновки

На основі проведеного порівняльного аналізу найбільш поширених ЕС та СНЛВ для оцінки ризиків інформаційної безпеки тестової ІТС встановлено, що система нечіткого логічного виводу має більше можливостей для настройки параметрів (як на підготовчому етапі, так і в процесі оцінювання ризиків ІБ), дозволяє оперувати якісними і кількісними даними і може замінити або доповнити CRAMM в процесі оцінки ризиків ІБ прикладних систем.

Література

1. Архипов О.Є. Оцінювання ризиків інформаційної безпеки: міжнародні стандарти та українське законодавство / Архипов О.Є., Кущ С.М., Шутовський В.О. // Інформаційні технології та комп'ютерна інженерія, №3, 2011. — С. 60—68.

2. Wayne Jansen. Directions in Security Metrics Research , NISTIR 7564, April 2009 [Електронний ресурс] // NIST.gov - Computer Security Division - Computer Security Resource Center [сайт] / Wayne Jansen ; Computer Security Division , Information Technology Laboratory , National Institute of Standards and Technology — Режим доступу: http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf (16.04.2012). — Назва з екрану.

3. Ручкин В.Н. Универсальный искусственный интеллект и экспертные системы / В.Н. Ручкин, В.А. Фулин. — С-П.: «БХВ-Петербург», 2009. — 240 с.

4. Питер Джексон. Введение в экспертные системы / Питер Джексон. — М.: «Вильямс», 2001. — 624 с.

5. Information technology — Security techniques — Information security management systems — Requirements: ISO/IEC 27001:2005. — [Чинний від 15-10-2005]. — Женева: [б.в.], 2005. — 42 с. — (Міжнародні стандарти ISO/IEC).

6. CRAMM User Guide. Issue 5.1 July 2005 / [інструкція / б.а.] — [б.в.], 2005. — 459 с.

7. Microsoft Security Assessment Tool [Електронний ресурс] // Microsoft Corporation [сайт] — Режим доступу: http://www.microsoft.com/download/en/details.aspx?id=12273 #overview (16.04.2012). — Назва з екрану.

8. Корченко А.Г. Построение систем защиты информации на нечетких множествах / Корченко А.Г. – К.:«МК-Пресс», 2006. – 316 с.

9. Gary Stoneburner. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology: NIST SP 800-30 [Електронний ресурс] // NIST.gov - Computer Security Division - Computer Security Resource Center [сайт] / Gary Stoneburner, Alice Goguen, and Alexis Feringa; Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology — Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (16.04.2012). — Назва з екрану.

10. Шутовський В.О. Розробка адаптативного алгоритму кількісної оцінки ризиків з використанням методів нечіткої логіки / Шутовський В.О. // VI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики». Збірка тез доповідей. Частина 2. — К.: 2008. — С. 71 — 72.

Кущ С.М., Шутовський В.О. ***Використання експертних та нечіткологічних систем для оцінки ризиків інформаційної безпеки ІТС.*** *Одним з важливих етапів в процесі розробки та експлуатації захищених інформаційно-телекомунікаційних систем є оцінка ризиків. У статті розглядається застосування експертних та нечіткогологічних систем для оцінки ризиків інформаційної безпеки ІТС. Для тестової ІТС проведено оцінку ризиків ІБ з використанням експертних систем CRAMM та MSAT та нечіткої експертної системи. Здійснено порівняння результатів та запропоновано рекомендації по застосуванню експертних та нечіткологічних систем при оцінці ризиків ІБ ІТС.*

Ключові слова*: інформаційна безпека, оцінка ризиків, експертні системи, нечітка логіка.*

Кущ С.Н., Шутовский В.О. ***Применение экспертных и нечеткологических систем для оценки рисков информационной безопасности ИТС.*** *Одним из важных этапов в процессе разработки и эксплуатации защищенных информационно-телекоммуникационных систем является оценка рисков. В статье рассматривается применение экспертных и нечеткологических систем для оценки рисков информационной безопасности ИТС. Для тестовой ИТС проведена оценка рисков ИБ с использованием экспертных систем CRAMM и MSAT, а также нечеткой экспертной системы. Осуществлено сравнение результатов и предложены рекомендации по применению экспертных и нечеткологических систем при оценке рисков ИБ ИТС.*

Ключевые слова*: информационная безопасность, оценка рисков, экспертные системы, нечетка логика.*

Kushch S.M. Shutovskyi V.O. ***Expert and fuzzy systems application for information security risks assessment of information and telecommunication systems.*** *The risks assessment is one of the main stages during the development and maintenance processes of the secure information and telecommunication systems (ITS). The expert and fuzzy systems application for information security risks assessment of information-telecommunication systems is considered in this paper. The risks assessment is held for the sample ITS using CRAMM and MSAT expert systems and fuzzy expert system. The results are compared. Recommendations are given for expert and fuzzy systems application during information security risks assessment.*

Keywords*: information security, risks assessment, expert systems, fuzzy logic.*