УДК 004.056.55

Застосування експертних систем у сфері аудиту інформаційної безпеки

Попов І.С., магістрант
Науковий керівник – аспірант Хох В.Д.
Центральноукраїнський національний технічний університет, м. Кропивницький

В сучасному світі інформація набуває великого значення. Викрадення чи пошкодження інформації може призвести до серйозних наслідків (як мінімум до матеріальних втрат), тому актуальною є проблема її захисту. Використання експертних систем (ЕС) може значно спростити спеціалістам з захисту інформації їх завдання. Експертні системи широко застосовуються у багатьох галузях, в тому числі й інформаційній безпеці. Оскільки ЕС ефективніше працюють у більш вузьких напрямах, вони створюються для вирішення конкретних, спеціалізованих, задач.

Експертні системи забезпечують можливість проведення оцінки ефективності захисту інформації на передпроектній стадії створення систем захисту інформації шляхом проведення аудиту інформаційної безпеки для визначення відповідності інформаційних систем вимогам безпеки. Типове оцінювання ефективності захисту інформації включає: підготовку вхідних даних, проведення контролю реалізації вимог, розрахунок показників оцінки стану системи захисту інформації.

Системи, які включають функціонал для аналізу налаштувань фаєрвола, на додачу до своїх правил, повинні отримувати список доступу та опис топології мережі. Розпізнавання потоку дозволених даних є базовою проблемою в аналізі списку доступу. Тому для успішної роботи таким системам необхідно знати відповідь на наступні запитання:

- Які сервіси доступні на даному хості?
- Чи даний хост доступний з іншого джерела?
- Який вид трафіку дозволений?

На додачу, експертні системи можуть розпізнавати загальні проблеми конфігурації та помилки. Наприклад:

- Фаєрвол не блокує прямі передачі (пакети, призначені для іншої адреси з під'єднаної мережі).
- Недостатнє запобігання підміни адрес як для вхідних, так і вихідних пакетів.
- DNS-сервер досяжний лише через протокол UDP (зазвичай залишається непоміченим, оскільки працює в 99% випадків) [1].

Зазвичай, для експертних систем аудиту інформаційної безпеки вхідні дані фільтруються та перетворюються у зрозумілу для ЕС форму, а вже після цього система починає обробку даних. Прикладом обробки вихідних

даних може бути система AudES [2], в якій всі можливі порушення, які було виявлено, відображаються, зберігаються та очікують рішення аудитора. Разом з цими даними зберігається й уся необхідна інформація - команди, ресурси та, найголовніше, відповідні рекомендації рішень для аудитора, які він повинен прийняти відповідно до вказівок аудиту безпеки. Після завершення консультації, аудитор може отримати копію результатів. На додачу, кожна консультація записується в окремий файл, який пізніше може бути використаний для відтворення консультації чи перевірки минулих аудитів [3].

Застосування нечіткої логіки в таких ЕС дозволяє охарактеризувати нечітко визначені змінні, визначити зв`язок між змінними, що базуються на знаннях експертів та використовувати їх для обчислення результатів. Використання нечіткої логіки в ЕС достатнє для емуляції прийняття рішень експертом [4, 5].

Перевагами експертних систем є те, що рівень їх знань не знижується, може передаватись, відтворюватись та підвищуватись; зниження ймовірності виникнення людського фактору; вартість розробки компенсується низькою вартістю використання.

Недоліком експертних систем є те, що вони не надто добре пристосовані до навчання новим правилам і концепціям. Використання експертних систем у більшості випадків дозволяє відмовитись від висококваліфікованих експертів, але передбачає наявність спеціаліста більш низької кваліфікації.

Таким чином, експертні системи можна розглядати як інструмент для підвищення інтелектуальної потужності в даній предметній області.

Список літератури

1. Pasi E. An expert system for analyzing firewall rules / E. Pasi, Z. Jukka. // Helsinki University of Technology. – 2001. – №1. – С. 1–8.

2. Kanatov M. Expert systems for Information Security Management and Audit. Implementation phase issues / M. Kanatov, L. Lyazzat, B. Bagdat. // SCIS&ISIS. – 2014. – №14. – С. 896–900.

3. Tsudik G. AudES - an Expert System for Security Auditing / G. Tsudik, R. Summers. // IAAI Proceedings. – 1990. – №1. – С. 221–232.

4. Кущ С. Використання експертних та нечіткологічних систем для оцінки ризиків інформаційної безпеки інформаційно-телекомунікаційних систем / С. Кущ, В. Шутовський. // Вісник Національного технічного університету України. – 2012. – №50. – С. 114–120.