Крок 4. Порівнюємо $\mu_D^i(RMSE)$ з попереднім значенням $\mu_D^{i-1}(RMSE)$.

Крок 5. Якщо $\mu_D^i(RMSE) < \mu_D^{i-1}(RMSE)$, то призначається нове значення коефіцієнта p, якщо $\mu_D^i(RMSE) > \mu_D^{i-1}(RMSE)$, те значення коефіцієнта p залишається без змін.

Таким чином, отриманий модифікований метод оптимізації декодування багатокомпонентних турбо кодів за рахунок додаткового використання показника невизначеності й функцій приналежності для прийняття рішень при розрахунку логарифмічних відносин функцій правдоподібності про передані біти інформаційної послідовності в алгоритмах декодування кожного компонентного декодера турбо кода.

Результати імітаційного моделювання безпроводової системи передачі даних з турбо кодами показали, що використання запропонованого методу дозволяє поліпшити їхні характеристики достовірності.

Література

1. Berrou C. Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes / C. Berrou, A. Glavieux, P. Thitimajshima // Proc. Int. Conf. On Commun., May 1993. – 1993. – P. 1064 - 1070.

2. Woodard J. Comparative Study of Turbo Decoding Techniques: An Overview / J. Woodard, L. Hanzo // IEEE Transactions on Vehicular Technology. – 2000. – Vol. 49, No. 6. – P. 2208 - 2232.

3. Hanzo L. MIMO-OFDM for LTE, WiFi and WiMax. Coherent versus Non-coherent and Cooperative Turbo-transceivers / Hanzo L., Akhtman Y., Wang. L. – New York: John Wiley & Sons, 2011. – 658 p.

УДК 004.056.53

ВИКОРИСТАННЯ МЕРЕЖ ПЕТРІ ДЛЯ ОЦІНКИ РИЗИКУ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ

П. С. Давиденко

Чернігівський національний технологічний університет

Методи , які використовуються в сучасних системах виявлення вразливостей (СВВ) є досить ефективними, якщо відомі точні характеристики атаки або загрози для інформаційної безпеки (ІБ). Проте тактика комп'ютерних атак на інформаційні системи (ІС) і, зокрема, мережеві варіанти атак постійно змінюються, наприклад, з появою нових технологій GPRS, Wi-Fi та ін. В подібних ситуаціях першочергове значення

набуває вміння скористатися доступною інформацією про всі потенційні загрози ІБ .

На сьогоднішній день існує багато робіт, які розкривають різні підходи до моделювання атак: мережі Петрі, метод аналізу зміни станів, емуляція вторгнень в послідовному і паралельному режимах, причинно-наслідковий модель, концептуальні моделі комп'ютерних вторгнень, описові моделі мережі і зловмисників, структурований опис на базі дерев, моделювання "виживання" комп'ютерних систем, об'єктно-орієнтоване дискретне подієве моделювання, модель запит / відповідь для комп'ютерних атак, ситуаційне обчислення і цілеспрямований виклик процедур, використання графів атак для аналізу вразливостей тощо.

Одним з найважливіших показників ефективності функціонування ІС є захищеність, поряд з такими показниками як надійність, відмовостійкість, продуктивність і т. д. Під захищеністю ІС зазвичай розуміють ступінь адекватності реалізованих в ній механізмів захисту інформації від існуючих в даному середовищі функціонування ризиків [1], пов'язаних із здійсненням загроз безпеки , що порушують такі властивості інформації, як конфіденційність, цілісність і доступність.

Типова методика включає використання наступних методів [2]:

• дослідження вхідних даних ІС;

• оцінка ризиків, пов'язаних із здійсненням загроз безпеки щодо ресурсів ІС;

• аналіз механізмів безпеки організаційного рівня і політики безпеки організації щодо забезпечення режиму інформаційної безпеки, а також їх адекватності існуючим ризикам;

• ручний аналіз конфігураційних файлів маршрутизаторів, міжмережевих екранів і проксі-серверів, які здійснюють управління міжмережевими взаємодіями, поштових і DNS серверів, а також інших критичних елементів мережевої інфраструктури.

На етапі експлуатації комп'ютерних систем для аналізу вразливостей і визначення рівня захищеності можуть використовуватися дві основні групи методів: пасивні та активні. Активне тестування системи захисту полягає в емуляції дій потенційного зловмисника по подоланню механізмів захисту. Пасивне тестування передбачає аналіз конфігурації операційної системи (ОС) і програм за шаблонами з використанням списків перевірки. Тестування може проводитися вручну, або з використанням спеціалізованих програмних засобів. Існує безліч систем аналізу захищеності (САЗ), що функціонують на етапі експлуатації, наприклад, Retina, Internet Scanner, CyberCop Scanner, Nessus Security Scanner тощо. Їх основними недоліками є:

1) відсутність відповіді на питання: "Які помилки в політиці безпеки були виявлені в процесі сканування?";

2) використання активного аналізу вразливостей для функціонуючої системи може призвести до порушення працездатності окремого сервісу або системи в цілому і т.д.

Серед методів, що використовуються в СВВ, можна виділити два напрямки: одне спрямоване на виявлення аномалій в захищається системі, а інше - на пошук зловживань.

Традиційними способами забезпечити гарантований захист ІС в умовах впливу комп'ютерних атак здається малоймовірним. Недосконалість засобів захисту інформації призводить до того, що в реальних умовах застосування ІС невідомі атаки долають границі протидії і вчиняють деструктивний вплив на систему.

Наявність факторів невизначеності апріорних знань про характеристики сценарію інформаційних акцій порушника і засобах реалізації атак, складність процесів управління і захисту інформації ІС призводить до необхідності створення комп'ютерних моделей для оцінки захищеності ІС [3].

Модель аналізу ризиків інформаційної системи

Якість аналітичних моделей оцінки інформаційної безпеки ІС має обмежену точність та достовірність. Підвищення цих показників можливе при імітаційному моделюванні ІС за допомогою мереж Петрі [4].

Покажемо на прикладі використання розфарбованих мереж Петрі, модельованих у системі CPN Tools для побудови моделі аналізу ризиків інформаційної системи.

У системі моделювання CPN Tools розфарбовані мережі Петрі являють собою комбінацію графа мережі Петрі та мови програмування CPN ML, використовуваної для опису атрибутів елементів. Фішка розфарбованої мережі Петрі - елемент абстрактного типу даних, який зазвичай називається кольором [5].

Структурно модель оцінки ризиків ІС включає в себе елементи представлені на рис. 1.

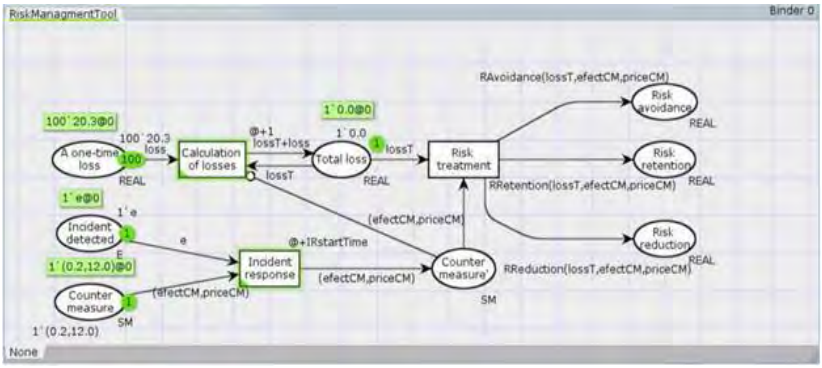

Рис. 1 - Модель обробки ризиків інформаційної безпеки

Представлена мережа Петрі (рис. 1) складається із 8 позицій та 3 переходів. Значення у позиції *A one time loss* сигналізує про кількість потенційних порушників та єдиноразові збитки від дій порушника, значення у позиції *Total loss* – загальні збитки до вжиття заходів захисту, наявність фішки у позиції *Incident detect* свідчить про факт, що інцидент виявлено через проміжок часу *IRstartTime*, фішка в позиції *Countermeasure* сигналізує про наявність заходу захисту проти загрози. Перехід *Incident response* використовується для демонстрації, що вживаються заходи для подолання інциденту, перехід *Calculatoin of losses* використовується для розрахунку загальних збитків, перехід *Risk treatment* використовується для обрання варіанта оброблення ризику.

У моделі використано три основних типи фішок: стандартний тип *REAL*, який описує рівень збитків від реалізації загроз; тип *SM*, який описує засоби захисту (а саме їх вартість та відсоток незахищеності, який залишиться після його впровадження); тип *E*, який в даній моделі використовується формально для демонстрації можливості факту виявлення інциденту безпеки.

Функція *RAvoidance* використовується для перевірки відповідності вимозі ухилення від ризиків, *RRetention* – утримання ризиків, *RReduction* – зниження ризиків.

Оголошення *IRstartTime*, яке визначає час від моменту настання інциденту до його розв'язання, тобто вживання заходів та/або засобів захисту, *RACriteria* – критерій прийняття ризиків, *Profit* – прибуток установи за певним процесом або в цілому.

Зміна *loss* описує збитки в результаті єдиноразової реалізації загрози, *lossT* – загальні збитки, які буде нанесено організації до моменту вжиття заходів захисту, *priceCM* – вартість засобів захисту інформації,

efectCM – небезпека, яка залишиться після використання даного механізму.

Висновок. Використовуючи мережі Петрі можна створити модель ідентифікації вразливостей ІС, що дають можливість отримати цілісне представлення про ризики ІБ незалежно від розмірів системи. Моделі, розроблені за допомогою мереж Петрі дають змогу підвищити рівень захисту ІС і зменшити рівень загроз та затрат ресурсів на наслідки вторгнень.

Література

1. Котенко Д.О. Метод оценки риска информационной безопасности на основе сценарного логико-вероятностного моделирования/ Котенко Д.О. – С.-Пб., 2010. – 16 с.
2. Вовченко В. В., Степанов И. О. Організаційні проблеми захисту інформації. - К.: Академія, 2003 .- 48-65с.
3. Стеценко, І.В. Моделювання систем: навч. посіб./ І.В. Стеценко ; М-во освіти і науки України, Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2010. – 399 с.
4. Кузьмук В.В. Сети Петри и моделирование параллельных процессов. – К.: ИПМЕ, 1985. – 64 с.
5.Зайцев Д.А. Исследование эффективности технологии MPLS с помощью раскрашенных сетей Петри/ Зайцев Д.А., Сакун А.Л. – http://teka.rulitru.ru/docs/2/1025/conv_1/file1.pdf

УДК 004.942:004.715

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ В ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ ТЕОРИИ КОНЕЧНЫХ АВТОМАТОВ

А.М. Хошаба
Национальный технический университет, Винница, Украина

Актуальность. Современные вычислительные системы (ВС) и используемые в них методы управления производительностью являются сложными и разнообразными, состоят из большого количества разнообразных элементов управления и учитывают множество различных факторов. Изучение таких систем актуально в связи с необходимостью анализа и оптимизации их функционирования, получения достоверной аналити- ческой модели изучаемых технологических процессов, формализации описаний для разработки программных продуктов. Поэтому, на