В процессе работы системы выполняется ручная и автоматическая проверка целостности данных и работоспособности средств комплекса. В случае сбоя или ошибки системы формируется текстовый отчет о проверке, в котором указываются места ошибок.

Комплекс содержит систему настроек и файлов обмена данными открытого формата, позволяющих адаптировать данную разработку к условиям различных диспетчерских пунктов. Передача комплекса пользователю в полном объеме дает возможность работникам диспетчерского пункта и службам ГО и ЧС предприятия самостоятельно изменять настройки и данные в случае изменения технологии производства или системы оповещения.

Выводы

Таким образом, создание информационной технологии и программно-аппаратного комплекса поддержки действий диспетчера в аварийных ситуациях позволяет ускорить выполнение необходимых в случае аварии операций и минимизировать возможность ошибки, связанной с психологическими и субъективными особенностями человека, а также получить в короткий срок объективный прогноз развития опасных событий

Список литературы: 1. РД-03-26—2007. Методические указания по оценке последствий аварийных выбросов опасных веществ [Текст] - Сер. 27. Вып. 6 / Колл. авт. - М.: НТЦ «Промышленная безопасность», 2008. - 124 с. 2. Братсерт, У.Х. Испарение в атмосферу. Теория, история, приложения [Текст] / У.Х. Братсерт. - Л.: Гидрометеоиздат, 1985. - 352 с.

Поступила в редколлегию 25.11.2010

УДК 519.179, 004.942

О.О. СУПРУНЕНКО**,** канд. техн. наук, доцент, Черкаський національний університет імені Богдана Хмельницького

МОДИФІКАЦІЯ ПІДСИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МЕРЕЖ ПЕТРІ

У статті розглядаються проблеми розробки підсистем захисту програмного забезпечення. Пропонується проводити моделювання, аналіз та модифікацію підсистеми захисту програми на моделі, побудованій на основі модифікацій мереж Петрі.
Ключові слова: підсистеми захисту, модель алгоритму програми, мережі Петрі.

В статье рассматриваются проблемы разработки подсистем защиты программного обеспечения. Предлагается проводить моделирование, анализ и модификацию подсистем защиты программ на модели, построенной на основе модификаций сетей Петри.
Ключевые слова: подсистемы защиты, модель алгоритма программы, сети Петри.

In the article considered the problems of the development of subsystems protection software. It is proposed to carry out simulation, analysis and modification of sub-programs on protection model based on modifications of Petri nets.
Keywords: security subsystem, the model algorithm programs, Petri nets.

Вступ

При проектуванні та реалізації комерційних програмних продуктів однією з основних задач є їх захист від несанкціонованого використання. При

випуску певної кількості екземплярів програмного продукту є потреба у створенні та коректній модифікації підсистем захисту інформації, оскільки при широкому використанні програмного продукту велика імовірність спроб зламу захисних механізмів, що може принести значні збитки компанії-виробнику. Окрім того, статичні модифікації захисних модулів слабкі до атак перетворення програмного коду, що вимагає застосування динамічних механізмів модифікації. Тому на даний час для захисту серійних програмних продуктів від нелегального копіювання та використання є потреба у створенні стійких підсистем ліцензійного захисту.

1. Виділення проблеми та постановка задачі

При створенні захисних підсистем широко застосовуються емпіричні підходи, які добре себе зарекомендували. Деякі з них – це апаратні ключі, активізація програмних продуктів через Internet, застосування методів та механізмів боротьби з відладкою та декомпіляцією [1]. Але час зламу цих систем останні часом скоротився і має термін від кількох годин до місяців. Підґрунтям для таких досягнень послужив швидкий розвиток сучасного апаратного забезпечення та вдосконалення методів динамічного дослідження програмних систем [2].

На сьогоднішній день назріла необхідність створення систем ліцензійного захисту, які використовують не тільки емпіричні підходи, але й мають теоретичне обґрунтування стійкості. Тому при виборі засобів розв‘язання цієї задачі потрібно обирати методи з розвиненою аналітичною базою. Крім того, необхідна розробка методів перетворення стійких алгоритмів захисту програмних продуктів для формування серійних підсистем захисту програм. Особливість таких алгоритмів полягає у перетворенні елементів даних у паралельних алгоритмічних структурах, які є частково-залежними MIMD-системами, без зниження рівня стійкості систем захисту.

2. Аналіз засобів розв‘язання задачі

Для моделювання захисних підсистем пропонується застосувати апарат мереж Петрі, який дозволяє відображати структурні і динамічні особливості паралельних алгоритмів, а також відслідковувати виникнення критичних ситуацій [3] при побудові та імітації роботи мережевих моделей.

В даній роботі пропонується створення програмного інструментального засобу для захисту від несанкціонованого використання програмних продуктів, який дозволяє будувати паралельні алгоритмічні моделі на основі безпечних мереж Петрі [3-4], для генерації підсистем захисту програм. В моделюючому середовищі створюється граф керуючої логіки [4], в якому реалізується алгоритм прихованого переходу на моделі, побудованій мережею Петрі. Граф керуючої логіки програмного продукту і захисного модуля поєднуються у єдину систему, що дозволяє протидіяти атакам на видалення захисного коду.

Структура модуля захисту формується на основі динамічної графової моделі. Механізм нарощування складності графа керуючої логіки дозволяє формувати різні за конструктивними ознаками захисні модулі. Теоретично обґрунтована неможливість розв‘язання задач, які належать до класу NP-повних задач, за прийнятний час дозволяє довести теоретично стійкість

отриманих модулів. Наприклад, пошук повного підграфа порядку k в графі, що вміщує певний гамільтонів шлях. В якості задач, розв‘язуваність яких ускладнена нерозвиненістю математичного апарату, можна розглядати задачу досяжності заданого переходу графа Петрі при невідомій початковій розмітці.

Використання динамічних структур даних і паралельної обробки дозволяє ускладнити задачу аналізу коду захисного модуля. Підвищення стійкості таких модулів обумовлено підвищеною складністю аналізу програми, що розміщує свої дані у динамічній області пам‘яті; швидкоплинністю процесів, що оперують цими даними; багатопоточною обробкою цих даних.

4. Приклад моделювання захисної підсистеми програмного продукту

Для побудови підсистеми захисту, яка дозволить перевіряти серійний номер і право володіння варіантом програмного продукту, застосовується модель на основі безпечної мережі Петрі [5]. Дана модель дозволяє при нарощуванні графа керуючої логіки контролювати його некритичність (рис. 1) за допомогою статичних та динамічних властивостей.

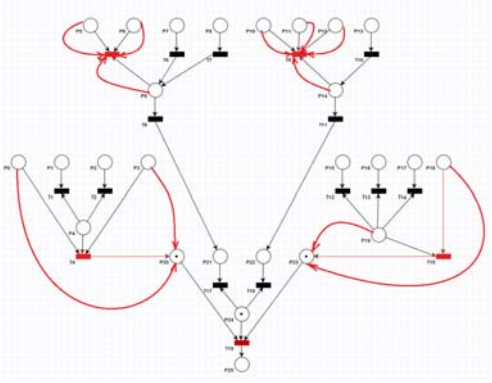

Рис. 1. Фрагмент моделі перевірки ключового слова, зображений безпечною мережею Петрі (червоними дугами показані шляхи передачі мітки)

Математично однозначний опис та перетворення графу (рис. 2.) на основі матриць інцидентності та вектор розмітки дає можливість перевіряти умови теоретичної стійкості системи захисту. Динамічне нарощування відлагодженого графа передбачене по елементах допоміжних гілок з використанням генератора випадкових чисел на основі ряду однорідних примітивів.

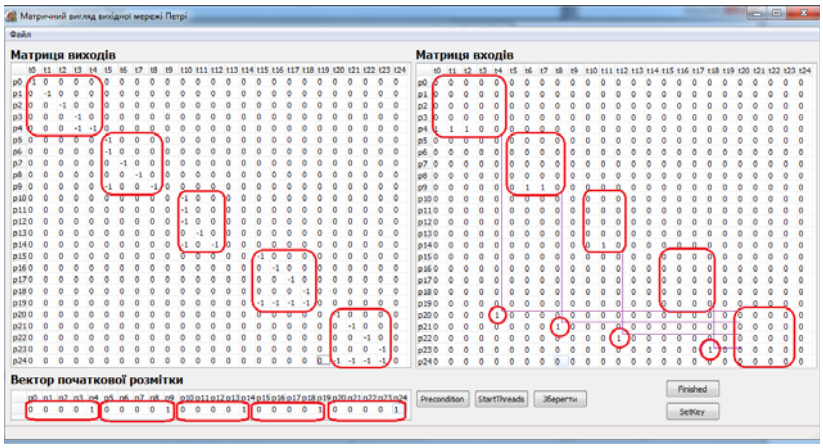

Рис. 2. Матричне подання топології моделі, побудованої на основі мережі Петрі

Розглянемо ділянку мережі Петрі (рис. 3), яка спрацьовує при подачі певного двійкового числа на вхід. Вхідними у даній ділянці мережі є вершини місць p_0, p_1, p_2 та p_3.

При початковій розмітці $p_0 = 1$, $p_1 = 0$, $p_2 = 1$, $p_3 = 1$ спрацюють переходи t_0 і t_1, наступними будуть розмічені вершини місць p_4, p_5 та p_6. За умов даної проміжної розмітки зможе спрацювати перехід t_2, а перехід t_3 буде закритий. Вершина місця p_7 моделює контрольну вершину, якщо вона матиме розмітку, то дозволить спрацювання одного з t_2 й t_3, якщо не матиме, ці вершини переходів будуть закриті.

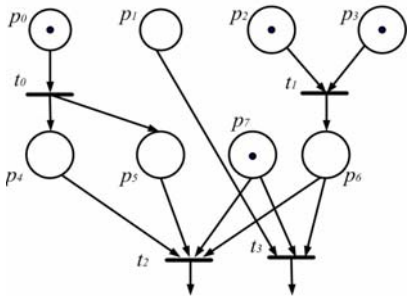

Рис. 3. Ділянка мережі Петрі, яка спрацьовує при початковій розмітці вершин місць (1011).

На рис. 4 представлений варіант нарощування мережі Петрі над вершиною місця p_0. Нарощування може відбуватися за допомогою двох типів примітивів – дозволяючих і забороняючих. За допомогою дозволяючого примітиву нарощування може відбуватися над вершинами p_0, p_2 та p_3 (рис. 3), які мають одиничну початкову розмітку. Забороняючий примітив потрібно під'єднувати до вершини місця p_1.

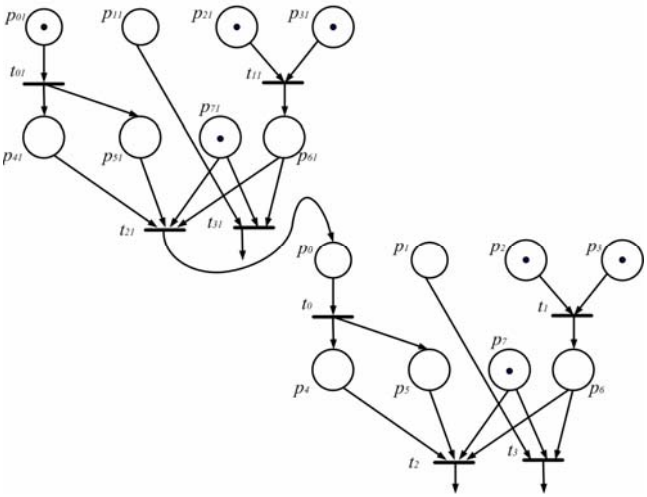

Рис. 4. Варіант нарощування мережі Петрі над вершиною місця p_0

Для створення надійних алгоритмів захисту на моделях, побудованих елементами мереж Петрі, необхідно нарощувати модель з врахуванням характеристики вершини та приєднуваного примітиву. Для забезпечення надійної роботи алгоритму необхідно вирішувати задачу досяжності певної розмітки μ_k з початкової розмітки μ_0. Ця задача може розв'язуватися на матричному поданні моделі та за допомогою дерева досяжності [5]. У матричному варіанті розв'язання задачі потрібно знайти цілочисельні розв'язки рівняння:

$$\mu_k = \mu_0 + (I_0 + I_v) \cdot x,$$

де I_0 - матриця вхідних функцій, I_v - матриця вихідних функцій. Це достатньо складна задача. Таким способом користуються у випадках, коли цілочисельні розв'язки можливо знайти за час, що не перевищує повне відпрацювання мережі – повний перебір. У інших випадках використовують дерево досяжності, на якому вирішують локальні задачі. Загальна задача пошуку ключа теж приводить до повного перебору. Таким чином, аналіз варіантів пошуку ключа у підсистемі захисту свідчить про надійність алгоритму при достатньо великих розмірах ключа, порядку 56 біт і більше.

5. Висновки

У представленій моделі підсистеми захисту програмних продуктів застосовані конструктивні примітиви на основі мереж Петрі. При нарощуванні

захисного коду у режимі конструктора модель дозволяє контролювати досяжність кінцевої розмітки, що забезпечує надійність функціонування захисту. Стохастична складова при формуванні остаточного графа ускладнює процес аналізу захисного коду. До того ж динамічний граф управляючої логіки захисного модуля поєднується з графом управляючої логіки програми, що дозволяє запобігти успішним атакам на видалення захисного коду.

Дані результати можливо застосовувати як основу для формування інструментарію формування ліцензійних підсистем захисту, аналіз коду яких є задачею підвищеної складності.

Список літератури: 1. Касперски К. Фрагмент из второго издания книги "Техника и философия хакерских атак 2000" [Электронный документ] http://www.wasm.ru/article.php?article = reg_ old . Проверено 23.09.2010 г. 2. Касперски К., Рокко Е. Искусство дизассемблирования. – СПБ: БХВ-Питер, 2008. – 896 с. 3. Кузьмук В.В. Сети Петри и моделирование параллельных процессов. – К.: ИПМЕ, 1985. – 64 с. (Препр. АН УССР, Институт проблем моделирования в энергетике; №17). 4. Доля А.В., Айрапетян Р.А. Защита программных продуктов с помощью сложных математических объектов на примере сетей Петри. // «Молодежь XXI века будущее Российской науки»: Тезисы докладов III Межрегиональной научнопрактической конференции студентов, аспирантов и молодых ученых. – Ростов-наДону: ЦВВР, 2005. – С. 26-27. 5. Романенко А.Ю., Супруненко О.О. Модификация серийных подсистем защиты программного обеспечения на основе сетей Петри. // Материалы IV Всероссийской конференции аспирантов и молодых учёных. – М.: МИРЭА, 2010. – С. 78-81.

Поступила в редколлегию 25.11.2010

УДК: 621.311.681.5

***Б.В. ФОМЕНКО*,** асистент, НТУУ «КПІ», м. Київ
***О.В. СТЕПАНЕЦЬ*,** аспірант, НТУУ «КПІ», м. Київ
***О.С. БУНКЕ*,** аспірант, НТУУ «КПІ», м. Київ

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ АВТОМАТИЧНОГО РЕГУЛЮВАННЯ ЗА РАХУНОК ВРАХУВАННЯ ОБМЕЖЕНЬ КЕРОВАНОГО СИГНАЛУ

У роботі запропоновано використання алгоритмів керування в нелінійних системах з врахуванням обмежень на керований сигнал. Представлені алгоритми на основі корекції роботи ПІ - та ІМС - регуляторів з компенсацією інтегрального насичення.
Ключові слова: нелінійні системи, ІМС-алгоритм, ПІ-регулятор з коректором, технологічні обмеження.

В работе предложено использование алгоритмов управления в нелинейных системах с учетом ограничений на регулируемый параметр. Представлены алгоритмы на базе коррекции работы ПИ - и ІМС - регуляторов с компенсацией интегрального насыщения.
Ключевые слова: нелинейные системы, ІМС-алгоритм, ПИ-регулятор с корректором, технологические ограничения.

In the article the use of control algorithms for nonlinear systems with output constraints has been proposed. There were presented algorithms based on the correction of the PI - and IMC - controllers with integral compensation of saturation.
Key words: nonlinear systems, IMC-algorithm, PI-controller with correction, output constraints.