

МЕТОД ПРОЕКТУВАННЯ ТА ВЕРИФІКАЦІЇ ФУНКЦІЙ КОМПЛЕКСІВ ЗАСОБІВ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

А.В. ЛЕНШИН

Пропонується комплексний метод проектування та верифікації комплексів засобів захисту інформації від несанкціонованого доступу. Аналізується підхід щодо створення та використання шаблонів для алгоритмів реалізації послуг безпеки у формальній нотації Паронджанова. Наводиться приклад застосування методу для розробки алгоритму реалізації послуги «відновлення після збоїв».

Ключові слова: захист від несанкціонованого доступу, НД ТЗІ 2.5-004-99, системний аналіз, дракон-схеми, нотація Паронджанова.

ВСТУП

Захист інформації, що обробляється в інформаційно-телекомунікаційних системах (ІТС), є завданням, що має вирішуватися за рахунок комплексного підходу, який передбачає застосування узгодженої сукупності процедурних, адміністративних та програмно-технічних рішень.

У разі створення комплексних систем захисту інформації (обов'язкова вимога законодавства у разі обробки в ІТС інформації з обмеженим доступом та/або інформації, яка відноситься до державних інформаційних ресурсів) мають використовуватися засоби технічного захисту інформації (ТЗІ): програмні, апаратні, апаратно-програмні.

Проектування комплексу засобів захисту (КЗЗ), що реалізовані у засобах ТЗІ, які використовуватимуться в складі КСЗІ, має здійснюватися з використанням критеріїв захищеності, що визначені у НД ТЗІ 2.5-004-99 [1].

Аналіз нормативної бази та сучасних публікацій вказує на відсутність методу, який би дозволяв здійснювати проектування КЗЗ від несанкціонованого доступу (НСД) із заданим рівнем гарантій та можливостями щодо протидії наперед визначеній множині загроз. На думку автора, особливо корисним цей метод має стати для розробників захищених від НСД компонентів обчислювальної системи, в яких функції захисту є додатком до основних — «бізнес» функцій продукту.

1. СУТНІСТЬ МЕТОДУ ПРОЕКТУВАННЯ ТА ВЕРИФІКАЦІЇ ФУНКЦІЙ КЗЗ ВІД НСД

Послідовність дій запропонованого у роботі методу згруповано у три етапи: «підготовка», «проектування» та «верифікація».

Дії, які виконуються на етапі «підготовка» здійснюються лише у ході розробки/адаптації метода, при цьому основними кроками етапу є:

- визначення набору критеріїв оцінки захищеності від НСД;
- первинна формалізація вимог критеріїв за рахунок структуризації їх вимог у вигляді множинних описів;
- розробка шаблонів для алгоритмів реалізації послуг безпеки при функціонуванні КЗЗ;

— визначення «типової» множини загроз безпеки, яким здатний протидіяти КЗЗ, спроектований за обраними критеріями [2];

— розробка правил уточнення множини загроз на етапі «проектування»;

— розробка правил формування програми випробувань із заданим рівнем покриття;

— визначення правил (функції) відображення множин загроз/послуг безпеки.

Виконання дій етапу «проектування» покладаються безпосередньо на розробника КЗЗ чи захищеного від НСД компонента обчислювальної системи, при цьому основними кроками етапу є:

- вибір (уточнення) підмножини загроз, яким має протидіяти КЗЗ розроблюваного засобу;
- відображення обраної множини загроз до переліку послуг безпеки;
- заповнення шаблонів послуг безпеки.

Дії, які виконуються на етапі «верифікація», можуть здійснюватися як у ході проведення попередніх випробувань, що проводяться розробником, так і під час проведення сертифікаційних випробувань (в Україні такими випробуваннями слід вважати Державну експертизу у сфері ТЗІ).

Основними кроками етапу «верифікація» є:

- формування програми випробувань за правилами, що є частиною методу;
- корегування типової методики випробувань з урахуванням особливостей КЗЗ, що розробляється;
- проведення випробувань та формування пропозицій з усунення викритих недоліків.

Окремо слід підкреслити, що в ході використання методу «автоматично» задовольняються умови, необхідні для забезпечення заданого рівня гарантій [1, 3].

2. ШАБЛони ДЛЯ АЛГОРИТМІВ РЕАЛІЗАЦІЇ ПОСЛУГ БЕЗПЕКИ ПРИ ФУНКЦІОНУВАННІ КЗЗ

Практичне застосування НД ТЗІ 2.5-004-99 під час розробки та експертизи КЗЗ свідчить, що форма подання специфікацій послуг є ускладненою і нечіткою [2]. Це призводить до неоднозначності у розумінні вимог розробниками КЗЗ та не лише негативно впливає на рівень захисту,

але і зумовлює додаткові фінансові витрати на усунення недоліків, викритих державними експертами з ТЗІ.

Зазначену проблему, у рамках застосування методу, пропонується вирішувати за рахунок розроблення шаблонів для алгоритмів реалізації послуг безпеки при функціонуванні КЗЗ. Шаблони є формалізованим поданням вимог нормативних документів, що регламентують порядок захисту від загроз НСД. В ході застосування такого підходу від розробника КЗЗ вимагається лише заповнити змінювані параметри залежно від особливостей продукту (середовища користувачів, технології обробки інформації, середовища використання тощо).

На основі висунутих критеріїв вибору способу опису алгоритмів, а саме: можливість формалізованого подання та наочність відображення, було обрано нотацію, яка запропонована Володимиром Паронджановим (відома під назвою: візуальна мова «Дракон») [4].

Обрана нотація базується на основі застосування двовимірних інформаційних оптичних сцен (діосцен). Для подання алгоритмів використовується множина ікон (дія, вибір, питання, адреса, петля циклу, петля силуету, вставка тощо) та макроікон (розвилка, перемикачі, цикл з передумовою, цикл з післяумовою тощо).

Застосування нотації Паронджанова та доступних у мережі Інтернет засобів розробки дозволяють автоматично генерувати вихідні програмні коди мовами програмування (C, C++,

Object Pascal, Assembler), з яких без додаткових зусиль можна отримати код, що виконується, із застосуванням стандартних компіляторів.

Незаперечною перевагою застосування нотації Паронджанова є наочність відображення алгоритмів та повністю формальне подання правил візуального структурного програмування.

На рис. 1 подано шаблон алгоритму реалізації послуги КА-2 «Базова адміністративна конфіденційність» у нотації Паронджанова (схема типу «Силует»). Окремо підкреслимо, що ідеологічною особливістю нотації Паронджанова є застосування носіїв подання інформації великого формату. Враховуючи обмеження сторінки збірника, на рисунку використані позначення (табл. 1), що погіршують ергономічний ефект від застосування нотації. Зацікавлений користувач зможе змоделювати приклад, використовуючи вільно доступні в мережі Інтернет засоби [5].

3. ПРИКЛАД ЗАСТОСУВАННЯ МЕТОДУ ДЛЯ ПРОЕКТУВАННЯ ФУНКЦІЙ КЗЗ, ЩО РЕАЛІЗУЄ ПОСЛУГУ ВІДНОВЛЕННЯ ПІСЛЯ ЗБОЇВ

Фахівці у сфері захисту інформації сходяться на думці, що однією із особливостей, яка зумовлена впровадженням інформаційних технологій у повсякденну діяльність людини, є зміщення акцентів із забезпечення конфіденційності інформації на підтримку безперервності роботи бізнесу. Враховуючи слабкість «людського чинника» цілком зрозумілим є прагнення розробни-

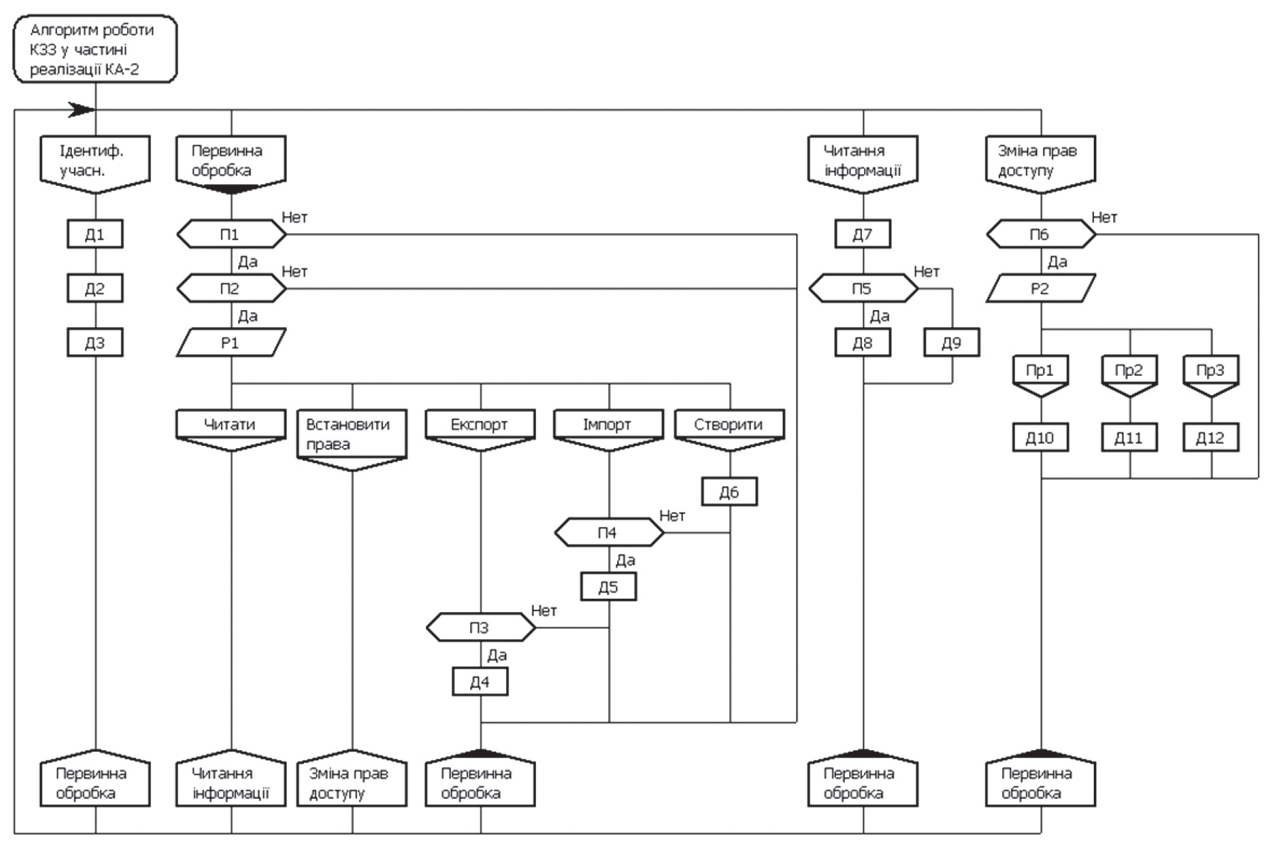


Рис. 1. Шаблон для алгоритму реалізації послуги КА-2

Таблиця 1

Використані на схемі позначення

Поз.	Розшифровка позначення
Д1	Визначити атрибути доступу для Користувача
Д2	Визначити атрибути доступу для Об'єкта
Д3	Визначити атрибути доступу для Процесу
Д4	Встановити для Об'єкта права доступу, що визначені політикою та виконати експорт
Д5	Виконати імпорт та встановити для Об'єкта права доступу, що визначені політикою
Д6	Створити новий об'єкт із правами доступу, що визначені політикою за замовчуванням
Д7	Зчитати матрицю доступу Користувачі/Об'єкти
Д8	Дозволити Користувачу прочитати вміст Об'єкта
Д9	Відмовити Користувачу у читанні вмісту Об'єкта
Д10	Змінити атрибути користувачів
Д11	Змінити атрибути захищених об'єктів
Д12	Змінити права на ініціювання процесів
П1	Чи має Користувач і/або групи до яких він входить право ініціювати Процес?
П2	Чи входить Об'єкт до множини об'єктів, для яких здійснюється розмежування доступу на читання?
П3	Чи має Користувач право на експорт?
П4	Чи має Користувач право на імпорт?
П5	Чи дозволено згідно з матрицею доступу читання вмісту Об'єкта для Користувача і/або групи до яких він входить?
П6	Чи є користувач уповноваженим користувачем?
Р1	Який тип має Запит?
Р2	Який підтип Запиту?
Пр1	Запит на зміну атрибутів доступу користувачів
Пр2	Запит на зміну атрибутів доступу об'єктів
Пр3	Запит на зміну атрибутів ініціації процесу

ків програмного та апаратного забезпечення до хоча б часткової автоматизації задач відновлення.

У нормативних документах з ТЗІ [1] закріплено послугу безпеки «відновлення після збоїв», що складається з трьох ієрархічно пов'язаних сукупностей вимог (рівнів):

- ручне відновлення (ДВ-1);
- автоматизоване відновлення (ДВ-2);
- вибіркове відновлення (ДВ-3).

Враховуючи те, що відмови та переривання в обслуговуванні можуть бути зумовлені як реалізацією об'єктивних, так і суб'єктивних загроз, обов'язковим елементом специфікації послуг «Відновлення після збоїв» є така вимога:

«Після відмови або переривання обслуговування КЗЗ повинен перевести комп'ютерну систему до стану, із якого повернути її до нормального функціонування може тільки адміністратор».

Результати проектування «окремого» варіанта реалізації послуги «Відновлення після збоїв», що використовує механізми захисту ОС

Windows, який розроблений на основі шаблону для послуги ДВ-1, наведено на рис. 2. Розглянемо його зміст детальніше.

Аналіз способів реалізації зазначених послуг у засобах ТЗІ, що мають позитивні експертні висновки Адміністрації Держспецзв'язку показав, що послуга ДВ найчастіше реалізується у системах, що мають трирівневу архітектуру або мають змогу працювати у привілейованому режимі (режимі ядра). Такі системи мають характерну ознаку: функціонування захищеного компонента в окремому домені виконання. Переважна більшість програм, для яких необхідно створити КЗЗ, не використовують драйвери та не працюють у режимі ядра. При цьому, міркування безпеки вимагають запускати ці програми від облікового запису з обмеженими правами.

Застосування шаблону для алгоритму реалізації послуги дозволило запропонувати альтернативний розв'язок зазначеної проблеми за рахунок висунення припущень щодо середовища використання продукту: *«При інсталяції програмного забезпечення адміністратором мають бути здійснені налаштування, що забезпечать реалізацію заданої політики розмежування доступу (ПРД) до об'єктів, що зберігатимуть еталонну інформацію щодо стану об'єкта захисту».*

ПРД до об'єктів, які зберігатимуть еталону інформацію подамо у вигляді таких правил:

— КЗЗ повинен мати право записувати та читати інформацію, що пов'язана з подіями безпеки;

— користувач, від імені якого запущено програму, не повинен мати право на зміну еталонної інформації.

Відомо, що для окремих категорій об'єктів, які підлягають захисту (каталоги, файли, елементи реєстру), механізми операційних систем з лінійки Windows дозволяють розділити право на запис та право на дописування інформації. Скориставшись цим у процесі інсталяції, можна призначити права доступу (засобами Windows) до файла (який буде сховищем еталонної інформації), що дозволять реалізувати задану політику розмежування доступу.

ВИСНОВКИ

Розроблений метод за рахунок використання методів системного аналізу при формалізації та верифікації вимог із захисту від НСД та застосування нотації Володимира Паронджанова (схеми типу «Силует») для опису шаблонів та алгоритмів функціонування КЗЗ дозволяє:

- розробити шаблони для алгоритмів реалізації послуг безпеки при функціонуванні КЗЗ;
- генерувати код програмних продуктів;
- задовольняти вимоги гарантій рівня Г-3;
- проводити випробування КЗЗ із наперед-визначеним ступенем покриття.

Подальшим завданням є розробка програмного засобу проектування КЗЗ на основні запропонованого методу.

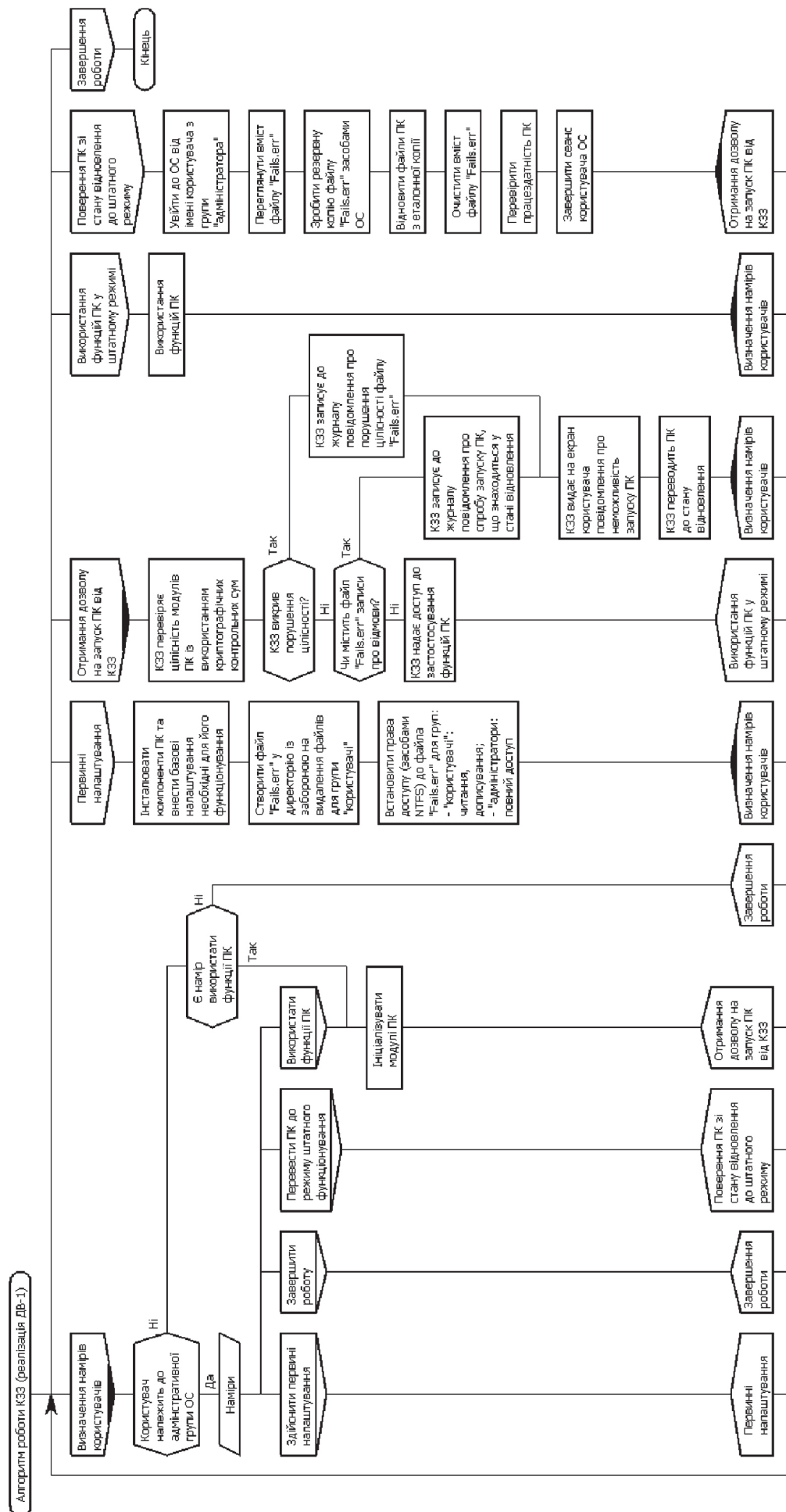


Рис. 2. Алгоритм роботи КЗЗ в ході реалізації послуги ДВ-1

Література

- [1] НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від НСД.
- [2] Леншин А.В. Метод формування функціональних профілів захищеності від несанкціонованого доступу / А.В. Леншин, П.В. Буслов // Науково-технічний журнал "Радіоелектронні і комп'ютерні системи". — Харків: ХАІ, 2010— Том 7. — С. 77—81.
- [3] ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.
- [4] Паронджанов В. Дружелюбные алгоритмы, понятные каждому. Как улучшить работу ума без лишних хлопот — М.: ДМК Пресс, 2010. — 466 с.
- [5] <http://drakon-practic.ru/>

Надійшла до редколегії 18.06.2014



Леншин Анатолій Валерійович, кандидат технічних наук, доцент, докторант кафедри «БІТ» ХНУРЕ. Наукові інтереси: захист від НСД, захист персональних даних, управління інформаційною безпекою.

УДК 681.3.06

Метод проектирования и верификации функций комплексов средств защиты от несанкционированного доступа / А.В. Леншин // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 328—332.

Предлагается комплексный метод к проектированию и верификации комплексов средств защиты информации от НСД. Анализируется подход к созданию и использованию шаблонов для алгоритмов реализации услуг безопасности в формальной нотации Паронджанова. Приводится пример применения метода для разработки алгоритма реализации услуги «восстановление после сбоя».

Ключевые слова: защита от несанкционированного доступа, НД ТЗИ 2.5-004-99, системный анализ, дракон-схемы, нотация Паронджанова.

Табл.: 01. Ил.: 02. Библиогр.: 05 назв.

UDC 681.3.06

The method of designing and verifying functions of trusted computing base for protection from unauthorized access /A.V. Lyenshyn // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 328—332.

A comprehensive approach to the design and verification of trusted computing base for protection from unauthorized access is offered. An approach to create and use templates for algorithms of implementing security services in a formal Parondzhanov notation is analyzed. An example of using the method for developing the algorithm of realizing the "failure recovery" service created with the proposed templates is given.

Keywords: protection from unauthorized access, technical information protection regulatory document 2.5-004-99, system analysis, dragon schemes, Parondzhanov notation.

Tab.: 01. Fig.: 02. Ref.: 05 items.