УДК 004.056, 004.75

В.Б. Дудикевич, І.Р. Опірський

Національний університет «Львівська політехніка», Львів

АНАЛІЗ МОДЕЛЕЙ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ДЕРЖАВИ

У статі представлено і проаналізовано моделі захисту інформації в інформаційних мережах держави. На основі аналізу загальної моделі процесу захисту інформації було представлено математичний вираз, який описує дану модель, а також визначено її недоліки. Проаналізовано загальну типову модель процесу захисту інформації з певним перекриттям загроз та модель системи захисту інформації з врахуванням взаємозв'язків системи захисту інформації, що дало змогу представити недоліки цих моделей та представити їхні аналітичні вирази. Розглянуті моделі повинні використовуватися на етапі проектування систем захисту інформації, коли ще не сформована архітектура системи, і необхідно дати попередню оцінку ефективності системи захисту інформації, яка проектується. Аналіз моделей моделі розмежування доступу до інформації (модель Харрісона, багаторівневого захисту, Кларка-Вілсона тощо) дозволив представити недоліки сучасних моделей захисту інформації в інформаційних мережах держави.

Ключові слова: *моделі захисту інформації, інформаційні мережі держави, загроза, несанкціонований доступ, багаторівневий захист, інформаційна система, джерело загроз.*

Вступ

Глобальне використання ПЕОМ та ІТС практично в усіх сферах життєдіяльності суспільства відкрило можливість масового доступу користувачів і зловмисників до інформації. У зв'язку з цим, на перший план виходить і активізується проблема створення високоефективних систем протидії і захисту.

Моделі захисту інформації є складовими частинами загального процесу моделювання. Моделювання системи заключається в побудові образу системи, адекватного (з точністю до цілей моделювання) системи, яка проектується, і в отриманні за допомогою побудованої моделі необхідних характеристик реальної системи. Таким чином, в самому загальному випадку, весь процес моделювання можна поділити на дві складові:

– побудова моделі;

– реалізація моделі з метою отримання необхідних характеристик системи.

Основне призначення моделей – це створення умов для об'єктивної оцінки загального стану інформаційної системи з точки зору міри уразливості або рівня захищеності інформації в неї. Необхідність в таких оцінках, зазвичай, виникає під час аналізу загальної ситуації з метою відпрацювання стратегічних рішень при організації захисту інформації.

Модель системи захисту інформації повинна відображати основні процеси, які протікають в цієї системі з метою оптимізації процесів захисту інформації. Такі процеси в самому загальному вигляді можуть бути представлені як процеси розподілу і використання ресурсів, які виділяються на захист інформації. По ступені узагальнення характеристик об'єкта дослідження моделі поділяються на загальні, часткові і локальні. До категорії загальних відносяться моделі, які дозволяють визначити (оцінити) загальні характеристики відповідних систем і процесів на відміну від часткових і локальних моделей, які забезпечують визначення (оцінку) будь-яких часткових або локальних характеристик системи або процесів. Тут не треба путати загальні моделі зі структурними, а локальні і часткові – з функціональними.

Метою даної роботи є проведення аналізу побудови сучасних моделей захисту інформації в інформаційних мережах держави.

Основна частина

Проаналізуємо приклади побудови основних моделей захисту інформації. Модель процесу захисту інформації представлена на рис. 1. У відповідності з класифікацією визначається як загальна, графічна (яка наглядно надає процес дослідження), математична (відображає принципи протікання процесу в математичній формі).

Аналітичний вираз, який описує цю модель, має вигляд:

$$\overline{W} = \sum_{i=1}^{n} P_i^{загр} \times \Delta q_i^{загр} \times P_i^{усун}, \qquad (1)$$

де $\overline{W}$ – показник якості функціонування системи захисту інформації; $P_i^{загр}$ – вірогідність появи загрози; $\Delta q_i^{загр}$ – загроза, яка вноситься в інформаційну систему; $P_i^{усун}$ – вірогідність усунення кож-

ної і-ї загрози. Недоліком такої моделі є складність визначення $P_i^{усун}$ системи захисту інформації, так як неможливо розглянути і точно визначити в цій моделі ймовірнісний показник надійної роботи системи захисту інформації. Також неможливо по цій моделі визначити вірогідність подолання порушником системи захисту інформації – тобто оцінювати вірогідність несанкціонованого доступу (НСД).

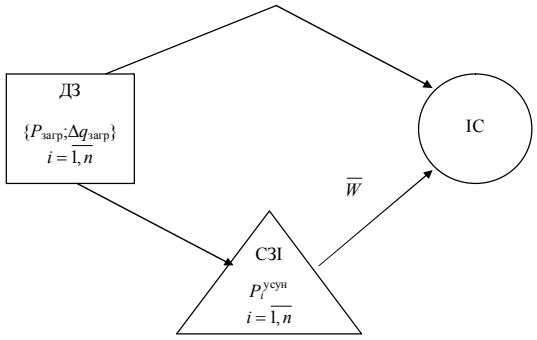

Рис. 1. Загальна модель процесу захисту інформації (ДЗ – джерело загроз, ІС – інформаційна система, СЗІ – система захисту інформації)

В якості розвитку приведеної вище моделі можна розглянути модель процесу захисту інформації, яка приведена на рис. 2.

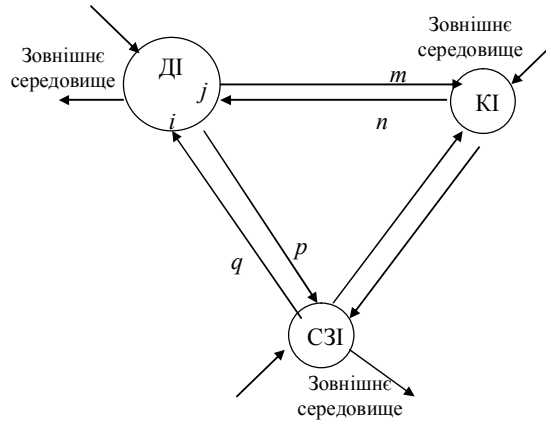

Рис. 2.Модель системи захисту інформації з врахуванням взаємозв'язків системи захисту інформації (СЗІ), джерела інформації (ДІ) та користувача інформації (КІ)

В цій моделі відображається взаємозв'язок самої системи захисту інформації з джерелом інформації і користувачем інформації. Причому в цій моделі враховується вплив зовнішнього середовища на усі складові (СЗІ, ДІ, КІ), які за своєю природою мають бути як природне так і штучне (дії порушника).

Аналітичним виразом цієї моделі є система

$$\begin{cases} A_{0j} = A_i W_{ij} W_{0j} = (A_n W_{in} + A_q W_{iq} + A_{i0} W_{i0}) W_{ij} W_{0j}; \\ A_{0q} = A_p W_{qp} W_{0q} = (A_j W_{jp} + A_n W_{pn} + A_{p0} W_{p0}) W_{qp} W_{0q}; \\ A_{0n} = A_m W_{nm} W_{0n} = (A_j W_{mj} + A_q W_{mq} + A_{m0} W_{m0}) W_{nm} W_{0n}. \end{cases} \quad (2)$$

Недоліком цієї моделі є то, що вона розкриває тільки взаємозв'язки між (учасниками) процесу захисту інформації, але не показує внутрішні процеси в самій системі захисту інформації, які в основному і впливають на якісну оцінку захисту інформації.

Одним з різновидів загальної моделі процесу захисту інформації є модель захисту інформації з повним перекриттям загроз, яка надана на рис. 3.

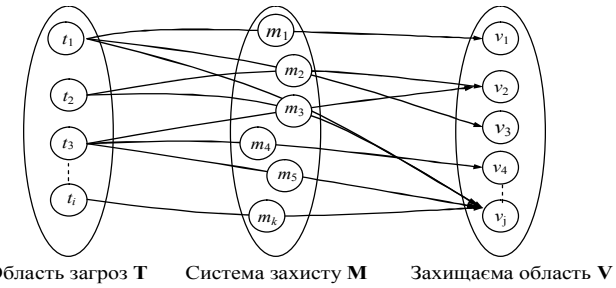

Рис. 3. Загальна типова модель процесу захисту інформації з певним перекриттям загроз

В цій моделі кожній загрозі, яка впливає на систему захисту, протиставиться механізм захисту зі складу системи захисту інформації.

Усі загрози повинні проходити тільки через механізм захисту, інакше немає користі від цієї моделі.

Подальшим удосконаленням цієї моделі є якісний розрахунок механізмів захисту з метою оцінки ефективності роботи системи захисту інформації.

Розглянуті моделі повинні використовуватися на етапі проектування систем захисту інформації, коли ще не сформована архітектура системи, і необхідно дати попередню оцінку ефективності системи захисту інформації, яка проектується.

В якості моделей системи захисту інформації (їх часткового випадку – по класифікації, яка приведена вище – функціональної моделі) виступають моделі аналізу розмежування доступу до інформації, які виділені в окремий клас.

Розглянемо найбільш відомі:

Модель Деннінга – ієрархічна багаторівнева модель захисту, в якій вводиться поняття концентрованих кілець захисту, в внутрішніх кільцях – самий жорсткий рівень безпеки і під час приближення до периферії – рівень безпеки знижується.

На рис. 4 представлена аналітична модель багаторівневого захисту інформації від загроз НСД.

В основу аналітичного виразу, який описує цю модель, покладена оцінка стійкості перешкод багаторівневого захисту (причому під ланцюгами контурів розуміють перешкоди, а товщина контуру відображає його стійкість):

$$P_{СЗІ} = 1 - \prod_{i=1}^{m} (1 - P_i), \quad (5)$$

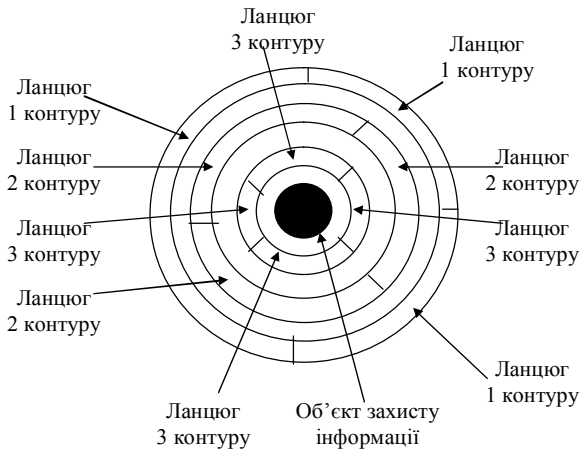

Рис. 4. Модель багаторівневого захисту від загроз НСД

$$P_i = P_i^{блок}(1 - P_{відм}), \qquad (6)$$

де $P_i^{блок}$ – вірогідність блокування і-ї перешкоди,

$$P_i^{блок} = t_н / T_{блок}, \qquad (7)$$

де $t_н$ – час подолання перешкоди порушником; $T_{блок}$ – час виявлення і блокування загрози НСД.

Вірогідність відмови системи захисту визначається наступним чином:

$$P_{відм} = e^{-\lambda t}, \qquad (8)$$

де λ – інтенсивність відмови технічних засобів захисту; t – час функціонування системи виявлення і блокування НСД.

Недоліком моделі є відсутність обліку можливої шкоди від впливу на інформацію і ефективність функціонування системи захисту.

Модель Белла і Ла-Падула – для побудови засобів розгородження прав доступу, вводяться поняття активних суб'єктів S та пасивних суб'єктів Q, які отримують різні права доступу.

Подальшим удосконаленням моделі Белла і Ла-Падула стала модель Біба – згідно якої усі суб'єкти і об'єкти попередньо розділяються на декілька рівнів доступу, а потім на їх впливи накладаються наступні обмеження: 1) суб'єкт не може визивати на виконання об'єкти з більш низьким рівнем доступу; 2) суб'єкт не може модифікувати об'єкти з більш високим рівнем доступу. Ця модель реалізована в захищеному режимі мікропроцесорів Intel 80386+ відносно рівнів привілеїв.

В моделі Харрісона мінімальна вимога до безпеки системи заключається в тому, що користувач, якій здійснює будь-яку операцію в системі, повинен знати, чи приведе виконання цієї операції до наступного переміщення привілеї доступу до суб'єкту, який цю привілею не мав, та не повинен мати. Харрісон показав, що базуючись на матричній моделі доступу, існує єдиний тип систем, який задовольняє вказаній вище вимозі – багатоопераційні системи (системи, які при виконані однієї високорівневої команди користувача виконують одну і тільки одну команду з базового набору команд). Недоліком такої моделі є те, що такі системи не можуть мати розповсюдження в силу своєї обмеженості і мають головним чином теоретичний інтерес.

Основою усіх розглянутих вище моделей аналізу розгородження доступу є обов'язкове використання диспетчера доступу, а сама система захисту уявляється тройкою:

$$Z = \langle S, Q, P \rangle, \qquad (9)$$

де S – суб'єкти, до яких відносяться користувачі та їх програми, а також народжені ними програми, процеси; Q – множина об'єктів (ресурсів) системи, які можуть запрошуватися суб'єктами; до об'єктів відносяться також програми, процедури, дані, томи, файли і пристрої; P – множина прав доступу суб'єктів до об'єктів.

Загальна модель системи захисту, яка враховує формулу (9), представлена на рис. 5.

Модель Гогена-Мезігера основана на теорії автоматів. Згідно її система при кожній дії переходить з одного дозволеного стану тільки в декілька інших. Суб'єкти і об'єкти в цієї моделі захисту розбиваються на групи – домени, і перехід системи з одного стану в інший виконується тільки в відповідності з таблицею дозволів, в якій вказано, які операції може виконувати суб'єкт. В цій моделі при переході системи з одного дозволеного стану в інший використовуються транзакції, що забезпечує загальну цілісність системи.

Сазерлендська (від англ. Sutherland) модель системи захисту робить акцент на взаємодії суб'єктів і потоків інформації. Також як і в попередній моделі, тут використовується машина станів з множиною дозволених комбінацій станів і набором початкових позицій. В цій моделі досліджується поведінка множини композицій функцій переходу з одного стану в інший.

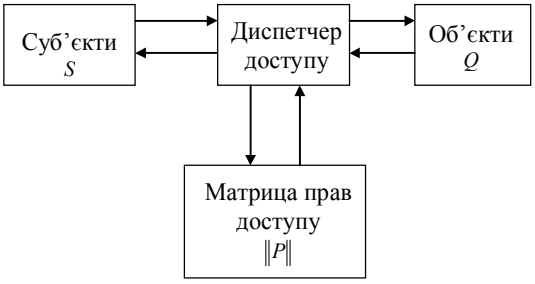

Рис. 5. Загальна модель системи захисту

Важливу роль в теорії захисту інформації грає модель захисту Кларка-Вільсона. Ця модель основана на постійному використанні транзакцій і старанному оформленні прав доступу суб'єктів до об'єктів. В цій моделі вперше досліджена захищеність третьої сторони в цій проблемі – сторони, яка підтримує усю

систему безпеки. Цю роль в інформаційних системах грає програма – супервізор. Крім того, в моделі Кларка-Вільсона транзакції вперше були побудовані по методу верифікації, тобто ідентифікація суб'єкта проводилася не тільки перед виконанням команди від нього, але і повторно після виконання. Це дозволило зняти проблему підміни автора в момент його ідентифікації. Модель Кларка-Вільсона вважається однією з самих удосконалених у відношенні підтримання цілісності інформаційних систем.

Ще на етапі раннього проектування багато дослідників ставлять перед собою проблему абстрактного уявлення системи захисту інформації, яка проектується, в залежності від цілей, задач, місця і обстановки, в якій вона буде функціонувати. Для цього важливо розібратися в існуючих підходах побудови різних моделей захисту інформації.

Модель системи захисту інформації повинна відображати основні процеси, які протікають в цієї системі з метою оптимізації процесів захисту інформації. Такі процеси в самому загальному вигляді можуть бути представлені як процеси розподілу і використання ресурсів, які виділяються на захист інформації.

Висновки

Моделі захисту інформації, які були проаналізовані, дозволяють систематизувати вивчення процесу моделювання, правильно підходити до оцінки моделей для подальшої побудови систем захисту інформації.

Список літератури

1. Михайлов С.Ф. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции / С.Ф. Михайлов, В.А. Петров, Ю.А. Тимофеев. – М.: Связь, 1995. – 56 с.

2. Голубенко О.Л. Політика інформаційної безпеки / О.Л. Голубенко, В.О. Хорошко, О.С. Петров, С.М. Головань, Ю.Є. Яремчук. – Луганськ: Вид: СНІ ім. В.Даля, 2009. – 300 с.

3. Єжова Л.Ф. Управління інформаційною безпекою. В 2-х томах / Л.Ф. Єжова, І.О. Мачалін, Я.В. Невойт, В.О. Хорошко. – К.: Вид. ДУІКТ, 2011.

4. Малюк А.А. Информационная безопасность: Концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: Высшая школа, 2004. – 280 с.

5. Щеглов А.Ю. Защита компьютерной безопасности от несанкционированного доступа / А.Ю. Щеглов. – СПб., 2004. – 384 с.

6. Згуровський М.З. Основи системного аналізу / М.З. Згуровський, Н.Д. Панкратова. – К:ВНУ, 2007. – 544 с.

7. Козлова К.В. Кількісна оцінка захисту радіоелектронних об'єктів / К.В. Козлова, В.О. Хорошко // Захист інформації. – 2007. – №1. – С. 30-32.

8. Ленков С.В. Методы и средства защиты информации. В 2-х томах. Том 1. Несанкционированное получение информации / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко; под ред. В.А. Хорошко. – К.: Арий, 2008. – 464 с., ил.

Надійшла до редколегії 21.03.2016

Рецензент: д-р техн. наук, проф. Л.Т. Пархуць, Національний університет «Львівська політехніка», Львів.

АНАЛИЗ МОДЕЛЕЙ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СЕТЯХ ГОСУДАРСТВА

В.Б. Дудыкевич, И.Р. Опирский

В статье представлены и проанализированы модели защиты информации в информационных сетях государства. На основе анализа общей модели процесса защиты информации было представлено математическое выражение, которое описывает данную модель, а также определены ее недостатки. Проанализированы общую типичную модель процесса защиты информации с определенным перекрытием угроз и модель системы защиты информации с учетом взаимосвязей системы защиты информации, что позволило представить недостатки этих моделей и представить их аналитические выражения. Рассмотренные модели должны использоваться на этапе проектирования систем защиты информации, когда еще не сформирована архитектура системы, и необходимо дать предварительную оценку эффективности проектируемой системы защиты информации. Анализ моделей модели разграничения доступа к информации (модель Харрисона, многоуровневой защиты, Кларка-Вилсона и т.д.) позволил представить недостатки современных моделей защиты информации в информационных сетях государства.

Ключевые слова: *модели защиты информации, информационные сети государства, угроза, несанкционированный доступ, многоуровневая защита, информационная система, источник угроз.*

ANALYSIS OF MODELS OF INFORMATION SECURITY IN INFORMATION NETWORKS OF STATE

V.B. Dudykevich, I.R. Opirsky

The paper presents and analyzes a model of information security in information networks of the state. Based on the analysis of the overall process model of information security was presented a mathematical expression that describes this model as well as its shortcomings identified. Analyzed overall typical process model of information security threats with a certain overlap and model of information security system based on the relationship information security system, which allowed to present disadvantages of these models and submit them to the analytical expressions. These models should be used in the design phase of information security systems, has not yet been formed when the architecture of the system, and you need to give a preliminary assessment of the effectiveness of the protection of information designed. Analysis of models of models of access to information (Harrison model, multi-layered security, Clark-Wilson, etc.) allowed to present the shortcomings of modern models of information security in information networks of the state.

Keywords: *model of information security, information networks of the state, the threat of unauthorized access, multi-layered protection, information system threats.*