УДК 65.012.810

Н. Ю. Траченко

ДОСЛІДЖЕННЯ МЕТОДІВ СИНТЕЗУ МОДЕЛЕЙ БЕЗПЕКИ ЯК ЕЛЕМЕНТУ СТАНДАРТУ АУДИТУ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ISO/IEC 27007

Вінницький національний технічний університет

Анотація

У роботі розглянуто основні моделі безпеки та методи їх синтезу, серію стандартів ISO/IEC 27000 - Менеджмент інформаційної безпеки, стандарт аудиту менеджменту інформаційної безпеки ISO/IEC 27007 детально, визначено етапи загальної методики синтезу моделі політики безпеки та розглянуто приклад синтезу захищеної автоматизованої системи.

Ключові слова: інформаційна безпека, аудит систем менеджменту інформаційної безпеки, синтез моделей безпеки, політика безпеки, математична модель безпеки, модель системи, модель безпеки інформації системи.

Abstract

The main safety models and methods of their synthesis, ISO / IEC 27000 - Information Security Management, ISO / IEC 27007 Information Security Management Audit Standard are considered in detail, the stages of the general methodology for the synthesis of the security policy model are defined and the example of the synthesis of the protected automated system is considered.

Keywords: Information security, information security management systems auditing, synthesis of security models, security policy, the mathematical model of security, the model of system, the model of security of information of the system.

Вступ

Роль інформації суттєво зросла в сучасних умовах, тепер інформація – товар, який має свою цінність та не повинен потрапити до рук того, кому не належить. Оскільки під час роботи будь-якого підприємства у ньому циркулює інформація з різними режимами доступу, то варто уникнути неприємностей через неправильне поводження з інформацією із обмеженим доступом. Для цього проводиться аудит менеджменту інформаційної безпеки, який має теоретичні та практичні засади.

Основи синтезу моделей безпеки

Важливою проблемою теорії захисту інформації є проблема складності задачі вивчення (аналізу) систем захисту інформації. У сучасній теорії захисту інформації цю проблему розв’язують, застосовуючи метод ієрархічної декомпозиції складних систем. З використанням цього методу, загальну складну систему розкладають на низку рівнів ієрархії. При цьому, верхній рівень ієрархії складає політика безпеки, другий рівень – системи підтримки політики безпеки, третій рівень – механізми захисту, четвертий рівень – реалізація механізмів безпеки.[1]

Формальне визначення політики безпеки називають математичною моделлю безпеки.

Згідно з вимог нормативних документів у галузі захисту інформації в інформаційних системах, системи захисту інформації будують на основі математичних моделей захисту інформації. Використання цих моделей дозволяє теоретично обґрунтувати відповідність системи захисту інформації вимогам заданої політики безпеки. [2]

Враховуючи, що доказовий підхід є базовим для розроблення та перевірки якості сучасних систем захисту інформації, відповідно до нього можна визначити такі етапи загальної методики синтезу моделі політики безпеки (ПБ) інформаційно-комунікаційної системи (ІКС) :

1. Визначення загальних вимог до моделі політики безпеки ІКС, що захищається.
2. Визначення умов та обмежень, які мають бути враховані під час формування моделі ПБ.
3. Визначення основних властивостей системи, які впливають на безпечність (захищеність) її функціонування (визначення безпечного стану системи).

4. Вибір з існуючих та синтез нових моделей безпеки, що будуть використані як базові для формування моделі ПБ.

5. Формування та опис правил оброблення інформації, метою яких є збереження для системи її безпечного стану (доведення теореми безпеки). [3]

Синтез гарантовано захищеної автоматизованої системи

1. Створення моделі системи

Визначається модель $\sum$, що обробляє цінну інформацію. Час є дискретним $t \in N, N = \{1,2, \dots\}$.

S - суб'єкти системи;

O - об'єкти системи;

D - загальні ресурси системи;

O_t – множина об'єктів системи $\sum$ в момент t.

Розглянемо деякі математичні припущення.

Припущення 1. Якщо суб'єкт S активізований у момент t, то існує єдиний активізований суб'єкт S'в $\boldsymbol{S_t}$, який активізував S. У момент $t = 0$ активізовані тільки користувачі.

Лема 1. Якщо в даний момент t активізований суб'єкт, то існує єдиний користувач U , від імені якого активізований суб'єкт S, тобто існує ланцюжок

$$U \overset{\alpha}{\rightarrow} S_1 \overset{\alpha}{\rightarrow} S_2 \overset{\alpha}{\rightarrow} \dots \overset{\alpha}{\rightarrow} S_k \overset{\alpha}{\rightarrow} S. \quad (1)$$

Припущення 2. Функціонування системи $\sum$ описується послідовністю доступів множин суб'єктів до множин об'єктів у кожний момент часу $t \in \boldsymbol{N}$.

Лема 2. *Для кожного* $t \in \boldsymbol{N}$*, для кожного* $O \in \boldsymbol{O_t}$*,* $O \notin \boldsymbol{D}$*, існує єдиний користувач* U *такий, щ* $O \in O_t(U)o$.

2. Створення моделі безпеки інформації системи

Розглянемо питання безпеки інформації в системі та деякі математичні припущення.

Припущення 3. Якщо $O \in \boldsymbol{D}$, то доступи в $U_i \overset{\rho}{\rightarrow} * O$, $U_j \overset{\rho}{\rightarrow} * O$ за будь-яких $\boldsymbol{\rho_1}$ і $\boldsymbol{\rho_2}$ не можуть створити канал витоку.

Припущення 4. Якщо деякий суб'єкт S, $S \in \boldsymbol{D}$, активізований від імені користувача U_i (тобто $U_i \overset{\alpha}{\rightarrow} * O$), у свою чергу суб'єкту S наданий у момент t доступу до об'єкта O, то або $O \in \boldsymbol{D}$, або $O \in O_t(U_i)$, або система припиняє роботу і вимикається.

3. Моделювання умов виконання політики безпеки

На цьому етапі будується зручна для реалізації множина послуг більш низького рівня, що підтримують політику безпеки. Тобто, визначається множина умов, реалізованих у системі $\sum$ таких, що можна довести теорему про достатність виконання цих умов для виконання правил політики безпеки. [3]

4. Реалізація гарантовано захищеної автоматизованої системи

Даний етап є заключним, його суть полягає у створенні системи, в якій можна з достатнім рівнем впевненості підтримувати функції 1-3.

Висновок

Підхід, що був продемонстрований у підпункті «Синтез гарантовано захищеної автоматизованої системи» дає можливість переглянути особливості роботи реальних інформаційних систем через математичні моделі, що дозволяє виявити недоліки в політиках безпеки та створити гарантовано захищену інформаційну систему.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Національний технічний університет України «Київський політехнічний інститут». Основні методи захисту інформації в комп'ютерних системах [Електронний ресурс] / Національний технічний університет України «Київський політехнічний інститут» – Режим доступу до ресурсу: https://studfiles.net/preview/5992521/.

2. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов / П. Н. Девянин. – М: Горячая линия - Телеком, 2012. – 320 с.

3. Основи теорії захищених систем. – С. 154–167.

Наталія Юріївна Траченко — студентка групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: natalia.nt25@gmail.com

Науковий керівник: ***Анатолій Антонович Шиян*** — к.ф. – м. н., професор, Вінницький національний технічний університет, м. Вінниця

Nataliia Y. Trachenko — Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email : natalia.nt25@gmail.com

Supervisor: Anatoliy A. Shiyan — Ph. D. in Physical and Mathematical Sciences, Professor, Vinnytsia National Technical University, Vinnytsia