КЛАСИФІКАЦІЯ МОДЕЛЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Клочкова Д.Ю., Пшеничних С.В.

Кафедра «Інфокомунікаційної інженерії ім. В.В. Поповського»,
Харківський національний університет радіоелектроніки,
Україна

E-mail: diana.klochkova@nure.ua,
serhii.pshenychnykh@nure.ua

Abstract

The report considers models of information protection systems when designing a complex information protection system. An analysis of the existing classifications of models of information protection systems was carried out, and the most convenient classification of models of information protection systems was presented. For a more detailed study and study of models of information protection systems, it is suggested to use just such a classification.

При розгляді побудови комплексної системи захисту інформації важливо приділити увагу поняттю моделі. При цьому варто враховувати, що при побудові моделі системи захисту інформації, вона не копіює оригінал, а спрощує. Модель повинна бути досить загальною, щоб описувати реальні дії з урахуванням їх складності.

Кожна модель створюється для конкретної мети тому вона унікальна. Але так як всі моделі мають спільні риси, то це дає можливість поєднати їх всі в окремі групи для спрощення їх дослідження. Існує багато класифікацій, але однією з найбільш зручних є класифікація за наступними ознаками:

- спосіб реалізації моделі;
- характер процесів, що протікають в об'єкті;
- характер підходу до об'єкта, що моделюється;
- за призначенням досліджуваного об’єкта;
- за характером досліджуваного об’єкта.

Далі слід розглянути класифікацію за кожною ознакою.

За способом реалізації моделі. Згідно з цією ознакою моделі діляться на два великих класи: абстрактні моделі та матеріальні моделі.[1]

Нерідко в практиці моделювання присутні абстрактно-матеріальні моделі (змішані).

Абстрактні моделі являють собою певні конструкції із загальноприйнятих знаків на папері, іншому матеріальному носії або у вигляді комп'ютерної програми.

Абстрактні моделі, не вдаючись у зайву деталізацію, можна розділити на символьні та математичні.

Матеріальне моделювання засноване на застосуванні моделей, що представляють собою реальні технічні конструкції. Це може бути сам об'єкт або його елементи (натурне моделювання). Це може бути спеціальний пристрій - модель, що має чи фізичну, або геометричну подібність оригіналу.

Змішані моделі – це з'єднання знакових форм виразу процесів і явищ з матеріальними моделями. Для тієї частини операції, яку неможливо описати за допомогою математичного апарату, використовують матеріальну модель, тоді як інше моделюється у знаковій формі.

За характером процесів, що протікають в об'єкті. За цією ознакою моделі можуть бути детермінованими або стохастичними, статичними або динамічними, дискретними, безперервними або дискретно-безперервними.[1]

Детерміновані та стохастичні моделі, в яких відповідно відсутній та присутній вплив випадкових процесів.

Статичні та динамічні моделі служать для опису стану об'єкта в будь-який момент часу та поведінку об'єкта в часі.

Дискретні моделі відображають поведінку систем з дискретними станами. Безперервні моделі відповідно представляють системи з безперервними процесами. Дискретно-безперервні моделі будуються тоді, коли дослідника цікавлять обидва ці типи процесів.

За характером підходу до моделювання об'єкта. Відповідно до цього ознакою моделі можуть бути: функціональними, структурними та інформаційними.[1]

Функціональна модель відображає сукупність виконуваних системою функцій. При функціональному моделюванні експеримент полягає в спостереженні за виходом модельованого об'єкта при зміні вхідних впливів

Структурне моделювання - це створення і дослідження моделі, структура якої подібна до структури об'єкта, що моделюється.

Інформаційна модель - модель об'єкта, представлена у вигляді інформації, яка описує суттєві для даного розгляду параметри і змінні величини про об'єкт.

За призначенням об'єкта дослідження. За цією ознакою розрізняють:[2]

- моделі загроз;
- моделі порушника;
- моделі політики інформаційної безпеки;
- моделі процесу захисту інформації;
- моделі систем захисту інформації;
- моделі систем управління доступом до ресурсів об'єкта.

Модель загроз – це формалізований або неформалізований опис методів і засобів здійснення загроз. Модель порушника – формалізований або неформалізований опис відповідних характеристик і поведінки порушника.

Модель системи захисту інформації повинна відображати основні процеси, які відбуваються в цій системі з метою оптимізації процесів захисту інформації.

Модель процесу захисту інформації відображає взаємодію між факторами, які впливають на інформацію, і протидіючими засобами захисту інформації, завершенням якого є визначений рівень захищеності інформації.

Модель політики інформаційної безпеки – формалізований або неформалізований опис відповідної політики, під якою розуміють сукупність законів, правил, обмежень, рекомендацій, інструкцій та інших нормативних актів, які регламентують порядок оброблення інформації.

Моделі систем управління доступом до ресурсів об'єкта, що захищається застосовують для вирішення задач аналізу та синтезу систем управління доступом до різного виду ресурсів об'єкта, насамперед до масивів даних або полів пристроїв запам'ятовування комп'ютерних систем

За ступенем узагальнення характеристик об'єкта дослідження моделі поділяють на загальні, часткові та локальні. До категорії загальних відносять моделі, які дають змогу визначити загальні характеристики відповідних систем і процесів, на відміну від часткових і локальних моделей, які забезпечують визначення будь-яких часткових або локальних характеристик системи або процесів.[2]

Отже, така класифікація дає загальне розуміння про моделі систем захисту інформації та може використовуватися для їх більш детального дослідження та вивчення.

Література

1. Боев, В. Д. Имитационное моделирование: учеб, пособие для вузов СПб. : Изд-во СПбДПУ, 2017.

2. Опірський І. Р. Класифікація моделей захисту інформації в інформаційних мережах держави. Науковий вісник Національного лісотехнічного університету України. Львів, 2015. Вип.25.10. С. 329 – 335.