МАТЕМАТИЧНА МОДЕЛЬ ОПТИМАЛЬНОГО ВИБОРУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

Пшеничних С.В., Добринін І.С., Клочкова Д.Ю.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

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

Abstract

The report examines and addresses the problem of optimal selection of information security measures against security threats in the design of a comprehensive information protection system within an information system. To choose security measures, a new efficiency indicator is proposed, allowing consideration of the implementation and operational costs of a particular measure, along with its capability to simultaneously protect against multiple threats. Based on this indicator, a criterion for the optimal selection of security measures against security threats is suggested for each information resource of the information system.

Практика показує, що проблема безпеки інформаційних технологій складна, різнопланова і пов'язана з вирішенням широкого спектра завдань, таких як побудова раціональних методів і моделей оцінки рівня безпеки інформаційних ресурсів в інформаційних системах (ІС) різного рівня, а саме – в системах управління органів державної влади, особливо силових структур, проведення аудита та експертиз стану безпеки інформаційно-телекомунікаційних систем з метою оцінки ефективності заходів щодо захисту інформації, розроблення ефективних апаратних і програмних засобів для реалізації алгоритмів методів і моделей систем безпеки інформаційних технологій [1, 2].

На сьогоднішній день ринок технологій та інструментів із кібербезпеки стійко зростає. З'являються новітні засоби безпеки автоматизованих робочих місць, інструменти мережного захисту, технології безпеки даних, веб-безпеки та захисту електронної пошти, програмні засоби для пошуку та аналізу вразливостей, а також системи управління доступом до конфіденційних даних.

В цих умовах одним з найважливіших завдань оптимальної побудови комплексної системи захисту інформації (КСЗІ) є вибір із множини наявних засобів такого їхнього набору, який дозволить забезпечити нейтралізацію всіх потенційно можливих інформаційних загроз із найкращою якістю та мінімально можливими витраченими на це ресурсами.

Для пошуку оптимальних варіантів, якщо завдання синтезу КСЗІ вдається формалізувати та представити параметри, що варіюються в числовій формі, застосовуються методи дискретного математичного програмування. Тоді задачу можна представити в такому вигляді:

$$F(X) \to \max_{X \in A}, \qquad (1)$$

де $F(X)$ - цільова функція, що математично виражає критерії оптимальності;

X – множина змінних, що варіюються та включає як параметри засобів захисту інформації, так і показники ефективності їхнього функціонування; A – множина допустимих значень X.

Основними методами вирішення задачі (1) є математичні методи скороченого перебору, а також різні наближення та евристичні методи (локальної оптимізації, еволюційні тощо). Достоїнством такого підходу є можливість використання відомих методів і алгоритмів оптимізації. Проте, для вирі-

шення цієї задачі необхідно визначити цільову функцію у формальному вигляді. Інформаційну систему, що захищається можна уявити як сукупність *M* критичних ресурсів під якими розуміється програмне, апаратне забезпечення, інформаційні потоки, та дані, що зберігаються в неї. Для кожного ресурсу визначаються наявні загрози безпеки, ймовірності їхньої реалізації P_{im} та можливі збитки C_{im} від їхньої реалізації. Далі розраховується ризик від реалізації *i*-ї загрози (R_{im}):

$$R_{im}=P_{im}\cdot C_{im}. \quad (2)$$

Після впровадження засобу захисту X_i величина ризику стане рівною:

$$R_{im}(X_i)=P_{im}(X_i)\cdot C_{im}. \quad (3)$$

З урахуванням вартості цього засобу захисту S_i пропонується використовувати наступний показник ефективності:

$$E_{im}(X_i)\left[\%\right]=\left(\frac{R_{im}-R_{im}(X_i)}{R_{im}}\cdot 100)\right)-\left(\frac{S_i\cdot A_{im}}{R_{im}}\cdot 100\right), \quad (4)$$

де A_{im}– булева змінна, яка вказує на повторне використання засобу захисту X_i, якщо він може забезпечувати захист інформації відразу від кількох загроз. Якщо $A_{im}=1$, то засіб захисту вибирається першій раз, інакше $A_{im}=0$. Результатом цього буде підвищення значення параметру $E_{im}(X_i)$.

Завданням оптимізації є вибір такого засобу захисту із множини *X*, для якого виконується умова:

$$X_{im}^{opt}=\arg\max E_{im}\left(X_i\right), \quad (5)$$

де X_{im}^{opt} – оптимальний засіб захисту інформації при реалізації *i*-ї загрози щодо *m*-го ресурсу, що захищається, $E_{im}(X_i)$ – ефективність засобу захисту (X_i) при реалізації *i*-ї загрози щодо *m*-го ресурсу, що захищається.

Загалом для комплексу засобів захисту *M* інформаційних ресурсів, які виявлені в ІС в ході попереднього обстеження (інвентаризації) для множини загроз *Y* вираз для параметра ефективності можна записати в наступному вигляді:

$$E(X)=\sum_{m=1}^{M}\sum_{i=1}^{Y}E_{im}(X_i). \quad (6)$$

Рішенням оптимізаційної задачі для КСЗІ буде знаходження складу комплексу засобів захисту $X_{opt}\in X$,для якого буде виконуватись умова:

$$X_{opt}=\arg\max_{X} E\left(X,Y,P,C,S,t\right) \quad (7)$$

де $E(X,Y,P,C,S,t)$ – узагальнений показник ефективності функціонування комплексу засобів захисту; $Y=\{Y_1,Y_2,\ldots,Y_i\}$ – множина загроз; $P=\{P_1,P_2,\ldots,P_i\}$ – ймовірності реалізації загроз; $C=\{C_1,C_2,\ldots,C_i\}$ – збитки від реалізації загроз; $S=\{S_1,S_2,\ldots,S_i\}$ – вартості реалізації засобів захисту; $t=T$ – час аналізу захищеності.

Згідно з цим критерієм, оптимальний КЗЗ повинен забезпечувати максимальне зменшення ризику при мінімальних витратах на його впровадження та експлуатацію.

Запропонована математична модель дозволяє поряд із вартістю сучасних засобів захисту враховувати їхні можливості щодо одночасної протидії довільній кількості загроз, що сприяє оптимальному вибору складу КЗЗ на етапі проектування КСЗІ в інформаційній системі.

Література

1. Домарєв В.В., Климчук Р.В. Тенденції розвитку методологічних, технологічних та організаційних основ створення систем інформаційної безпеки // Сучасний захист інформації. 2013. №1. С. 55-57.

2. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я. Ю. Усов. – Ніжин: ФОП Лук'яненко В. В., ТПК «Орхідея», 2019. – 144 с.