АНАЛІЗ МЕТОДІВ ОПТИМІЗАЦІЇ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Румянцева О.В., к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки,
кафедра Інфокомунікаційної інженерії ім. В.В. Поповського,
м. Харків, Україна
e-mail: olha.rumiantseva@nure.ua

Abstract. The report reviews well-known optimization methods that can be used to solve the problem of choosing from a set of available tools of such a set that will ensure the neutralization of all potential information threats with the best quality and the lowest possible cost of resources. The report also reviews issues related to the choice of performance indicators and optimality criteria for a comprehensive information security system. It also considers the evaluation of the effectiveness of the functioning of a comprehensive information security system, which is carried out based on the results of the analysis.

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

Відомо, що найефективніше завдання захисту інформації вирішуються у межах попереджувальної стратегії захисту, коли на етапі проектування оцінюються потенційно можливі загрози і реалізуються механізми захисту від них. При цьому на етапі проектування системи захисту інформації розробник, не маючи статистичних даних про результати функціонування системи, змушений приймати рішення про склад комплексу засобів захисту (КЗЗ) інформації, перебуваючи в умовах значної невизначеності.

Водночас прорахунки у виборі комплексу засобів захисту інформації на етапі проектування ведуть до невиправданого збільшення збитків від реалізації деструктивних впливів. Крім того, у процесі проектування системи захисту інформації на об'єкті інформатизації найбільш трудомісткими та найменш забезпеченими у методичному плані є етапи оцінки ефективності та вибору оптимального проектного варіанту.

Створення системи комплексного захисту вимагає тривалого часу, залучення великої кількості експертів. Термін служби комплексної системи захисту інформації є тривалим. Протягом терміну служби кілька разів може змінитись склад її технічних засобів. Виходячи з цього, одним з основних питань, які вирішуються розробником комплексної СЗІ, є оптимізація складу комплексу засобів захисту, що забезпечує збереження ефективності її функціонування протягом життєвого циклу. Одним з

найскладніших є завдання оптимізації складу засобів захисту на етапі проектування.

Розглядаючи завдання побудови оптимального КЗЗ у СЗІ як завдання проектування складного технічного об'єкта, її математичну постановку можна представити у наступному вигляді. Необхідно знайти безліч засобів захисту $X_{opt} \in X$ таке, що

$$X_{opt} = \underset{X}{arg\ extr}\, I(X, Y, t),$$

де $I(X,Y,t)$ – узагальнений показник ефективності функціонування комплексу засобів захисту.

Потрібно сформувати склад засобів захисту інформації з багатьох доступних, які забезпечують виконання всіх необхідних функцій за умови досягнення оптимуму обраного критерію та виконання відповідних обмежень. Крім того, такий набір засобів захисту повинен задовольняти вимогам нормативних документів та вимогам сумісності.

При цьому приймаються такі припущення та обмеження:

– час аналізу захищеності поставлено ($t = T$);

– безліч потенційно можливих загроз Y визначено і є кінцевим;

– зловмисник є інформаційним суб'єктом, здатним до навчання;

– витрати на експлуатацію КСЗІ постійні, а їх надійність абсолютна;

– випадки появи різних ненавмисних загроз є незалежними випадковими подіями.

У доповіді розглядаються відомі методи оптимізації, які можуть бути використані для вирішення завдання вибору оптимального складу засобів захисту інформації у КСЗІ, а також питання, що стосуються вибору показників ефективності та критеріїв оптимальності КСЗІ.

Як показник ефективності КСЗІ найчастіше використовується залишковий ризик реалізації загроз інформаційної безпеки, а критерій оптимальності визначається співвідношенням ефективності КСЗІ та вартості самого комплексу з урахуванням витрат на його експлуатацію та підтримання у робочому стані.

Оцінка ефективності функціонування КСЗІ здійснюється за результатами аналізу, що здійснюється за допомогою моделювання.

Список використаних джерел.

1. Горохов Д.Е. (2009). Методика оптимизации комплекса средств защиты на основе априорной оценки риска. Информация и безопасность, (4), 603 – 606.

2. Пиявский С.А. (2014). Простой и универсальный метод принятия решений в пространстве критериев «Стоимость–эффективность». Онтология проектирования, 3 (10), 89–102.