МАТЕМАТИЧНА ПОСТАНОВКА ЗАДАЧІ ОПТИМАЛЬНОГО ВИБОРУ ЗАСОБІВ ЗАХИСТУ ПРИ ПРОЄКТУВАННІ КОМПЛЕКСНОЇ СИСТЕМИ 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 discusses the mathematical formulation of the problem of optimal selection of information security measures in the design of a comprehensive information security system for an information technology facility. An analysis of existing approaches to assessing the effectiveness of information security systems is carried out, and a mathematical model for the optimal selection of the composition of security measures is proposed. To choose security measures, it is proposed to use an efficiency indicator that takes into account the costs of implementing and operating the respective security measure.

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 КСЗІ, 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.

На сьогоднішній день методичне забезпечення щодо комплектування КСЗІ засобами захисту для об'єктів інформатизації, у тому числі для телекомунікаційних систем, сформовано недостатньо повно. Вибір необхідного комплексу засобів захисту (КЗЗ) для забезпечення функціонування даної системи згідно нормативних документів здійснюється відповідно до категорії об'єкта [1, 2]. Але, побудова КСЗІ на основі використання нормативного підходу не дозволяє говорити про її оптимальність, тому, що не визначається ефективність та не враховується вартість конкретних механізмів захисту. Оцінка ефективності КСЗІ методом натурних випробувань пов'язана з певними труднощами

та не завжди можлива. Найчастіше вона визначається за результатами математичного моделювання. Таким чином, завдання розвитку та розробки методичного забезпечення щодо оптимального вибору складу КЗЗ на етапі проектування КСЗІ є дуже актуальним.

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

$$X_{opt} = \underset{X}{arg\,extr}\, E(X, Y, P, C, S, t), \quad (1)$$

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.

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;
- 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.

У роботі [3] як показник ефективності розробки КСЗІ використовується величина, яка дорівнює різниці між збитками, які вдалося запобігти та витратами на впровадження та експлуатацію засобів безпеки:

$$E = \sum_{i=1}^{K} \left(C_i - C_i^*\right) - \sum_{b=1}^{B} \left(S_b^{en} + S_b^{ek}\right), \quad (2)$$

де E - ефективність розробки КСЗІ, К – кількість загроз, C_i – величина збитків від реалізації і-ї загрози до впровадження КСЗІ, C_i^* – величина збитків від реалізації і-ї загрози після впровадження КСЗІ, В – кількість засобів захисту, $S_b^{вп}$ – витрати на впровадження b-го засобу захисту, $S_b^{ек}$ – витрати на експлуатацію b-го засобу захисту.

Але, за такого підходу не враховуються ймовірності реалізації загроз, що не дозволяє оптимальним чином вибрати адекватні методи і засоби захисту. Доцільно таким чином формувати КЗЗ, щоб витрати на безпеку були адекватні потенційним загрозам [4]. Подібна ситуація визначає необхідність оцінки та врахування ймовірностей реалізації загроз. Крім того, треба врахувати те, що сучасні засоби захисту здатні протидіяти одночасно декільком загрозам безпеки. Тому показник ефективності КСЗІ повинен враховувати крім витрат на впровадження та експлуатацію засобів захисту від загроз безпеки їх можливості щодо одночасного захисту від декількох загроз.

Література

1. НД ТЗІ 2.5-007-07. Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу 1. Чинний від 2007.12.12. Київ : Державна служба спеціального зв'язку України, 2007. 9 с.

2. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. 28.12.2012. Київ : Державна служба спеціального зв'язку України, 1999. 60 с.

3. Домарев В. В. Безопасность информационных технологий, системный подход. Санкт-Петербург : ТИД «ДС», 2004. 317 с.

4. Домарев В. В. Безопасность информационных технологий: Методология создания систем защиты. – Киев: Диасофт, 2002. – 688 с.