УДК 621.396:004.056.5

ОГЛЯД МЕТОДІВ ОПТИМІЗАЦІЇ СКЛАДУ КОМПЛЕКСУ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Румянцева О.В.
Науковий керівник - к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії ім. В.В. Поповського,
м. Харків, Україна
тел+38(099) 029-93-20, e-mail: olha.rumiantseva@nure.ua

The report reviews the known methods of optimization, which can be used to solve the problem of choosing the optimal composition of information security features in the created state firewall, as well as issues relating to the selection of performance indicators and criteria for the optimality of state firewall.

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 [1].

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 [2].

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

$$X_{opt} = \arg\left[\underset{X}{\text{extr}}\, I(X, Y, t)\right]$$

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. Методика оптимизации комплекса средств защиты на основе априорной оценки риска / Д.Е. Горохов // Информация и безопасность : регион, науч.-техн. журнал. Воронеж, 2009. Вып. 4. С. 603-606.

2. Пиявский С.А. Простой и универсальный метод принятия решений в пространстве критериев “стоимость–эффективность” // Онтология проектирования. 2014. № 3 (10). С. 89–102.