ОПТИМІЗАЦІЯ ВИБОРУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ОБМЕЖЕНОМУ БЮДЖЕТІ

Пшеничних С.В., Добринін І.С., Фукс М.А.

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

E-mail: serhii.pshenychnykh@nure.ua
ihor.dobrynin@nure.ua
maksymillian.fuks@nure.ua

Abstract

This report addresses the problem of optimal selection of information protection tools against security threats within an information system under a budget constraint. A mathematical formulation of the problem is presented, and the main stages of its solution are outlined. An efficiency metric is proposed for the selection of security tools, which allows for the consideration of implementation and operational costs for each specific tool, as well as its ability to protect against multiple threats simultaneously. Based on this metric, an algorithm for the optimal selection of security tools to counter threats for each information resource of the system is proposed.

Вступ

При проектуванні підсистем захисту інформації в інформаційних системах виникає завдання оптимального вибору комплекту засобів захисту від загроз безпеки при обмеженому бюджеті підприємства. На сьогоднішній день ринок технологій та інструментів із кібербезпеки стійке зростає. З'являються новітні засоби безпеки автоматизованих робочих місць, інструменти мережного захисту, технології безпеки даних, веббезпеки та захисту електронної пошти, програмні засоби для пошуку та аналізу вразливостей, а також системи управління доступом до конфіденційних даних.

У цих умовах одним із найважливіших завдань оптимального вибору складу системи захисту інформації (СЗІ) є вибір із множини наявних засобів такого набору, який дозволить забезпечити нейтралізацію всіх потенційно можливих інформаційних загроз із найкращою якістю та мінімально можливими витраченими на це ресурсами. Доцільно таким чином формувати комплект засобів захисту, щоб витрати на безпеку були адекватні потенційним загрозам. До уваги необхідно брати обмежені фінансові ресурси та принцип розумної достатності при побудові ефективної та дієвої СЗІ.

На сьогодні опубліковано значну кількість робіт в яких розглядаються питання вибору оптимального набору засобів кіберзахисту. Так, у роботі [1] показано можливість використання математичного апарату теорії ігор для обґрунтування прийняття рішення щодо вибору варіанту побудови СЗІ корпоративної мережі. Показано, що задача, яка розглядається, може бути віднесена до дуельної гри з нульовою сумою, гравцями якої є адміністратор мережі та потенційний зловмисник. Окреслені шляхи вирішення подібного класу задач з акцентом на ітеративний метод Брауна-Робінсон. У роботі [2], на основі критерія максимуму інтегрального показника ефективності, вирішується задача оптимального вибору засобів захисту інформації від загроз безпеки при проектуванні КСЗІ.

Згідно з чинними нормативними документами щодо побудови КСЗІ, вибір необхідного комплекту засобів захисту (КЗЗ) для забезпечення функціонування даної системи здійснюється відповідно до категорії об'єкта [3], [4]. Проте в жодній із документації не згадується про оптимізацію КСЗІ, про розумну достатність у побудові системи захисту інформації, не визначається ефективність та не враховується вартість конкретних механізмів захисту.

Метою дослідження є розробка математичної моделі оптимального вибору КЗЗ інформаційної системи від можливих атак при обмеженому бюджеті підприємства.

Математична постановка задачі

Для пошуку оптимальних варіантів застосовуються методи дискретного математичного програмування. Основними методами вирішення задачі є математичні методи скороченого перебору, а також різні наближення та евристичні методи (локальної оптимізації, еволюційні тощо). Перевагами такого підходу є можливість використання відомих методів і алгоритмів оптимізації.

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_{km} та можливі збитки C_{km} від їхньої реалізації. Далі розраховується ризик від реалізації *k*-ї загрози (R_{km}):

$$R_{km} = P_{km} \cdot C_{km}. \quad (1)$$

Після впровадження засобу захисту X_i величина ризику стане рівною:

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

В роботі [2] запропоновано використовувати наступний показник ефективності:

$$E_{km}(X_i)[\%] = \left(\frac{R_{km} - R_{km}(X_i)}{R_{km}} \cdot 100\right) - \left(\frac{S_i \cdot A_{im}}{R_{km}} \cdot 100\right), \quad (3)$$

де S_i– вартість засобу захисту;
A_{im}– булева змінна, яка вказує на повторне використання засобу захисту X_i, якщо він може забезпечувати захист інформації відразу від кількох загроз. Якщо засіб захисту вибирається першій раз, то $A_{im} = 1$, у іншому випадку – $A_{im} = 0$.

Цей показник відображає баланс між усуненим (завдяки використанню засобу захисту X_i) ризиком і вартістю цього засобу S_i (з урахуванням втрат на його впровадження та експлуатацію) для *m*-го інформаційного ресурсу в разі реалізації *k* -ї загрози. Він дозволяє врахувати можливості засобів захисту забезпечувати захист відразу від кількох загроз для декількох ресурсів інформаційної системи.

Завданням оптимізації є вибір такого засобу захисту із множини $\vec{X} = \{X_1, X_2, \ldots, X_B\}$, для якого виконується умова:

$$X_{km}^{opt} = \arg\max_{X_i \in \vec{X}} E_{im}(X_i), \quad (4)$$

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

За умови обмеженого бюджету S_{max} для комплексу засобів захисту (КЗЗ) для *M* інформаційних ресурсів інформаційної системи при множині загроз *K* вирішується оптимізаційна задача:

$$E(\vec{X}) = \sum_{m \in M} \sum_{k \in K} E_{km}(X_i) \rightarrow \max_{\vec{X} \in \Delta\vec{X}}, \quad (5)$$

$$\Delta\vec{X} : \sum_{i \in B} S_i \leq S_{max}, \quad (6)$$

де $\Delta\vec{X}$ – множина припустимих варіантів складу КЗЗ.

Рішенням оптимізаційної задачі для системи захисту буде знаходження складу комплексу засобів захисту $\vec{X}_{opt} = \{X_1, X_2, \ldots, X_N\}$, для якого буде виконуватись умова (5). Кількість засобів захисту *N* у складі КЗЗ буде визначатися з урахуванням можливостей конкретних засобів щодо протидії кільком загрозам.

Алгоритм вибору засобів захисту інформації

У роботі [2] для формування КЗЗ запропоновано алгоритм повного перебору. Хоча показник ефективності (3) враховує вартість придбання, впровадження та експлуатації засобів захисту, проте обмеження на загальну вартість КЗЗ не враховується. В умовах обмеженого бюджету необхідно знайти раціональний алгоритм формування КЗЗ, який задовольняє критерію (5) при заданому обмеженні (6).

Пропонується наступний алгоритм.

На першому кроці, при виборі засобу захисту для *m*-го ресурсу від *k*-ї загрози вибираємо засіб із максимальними можливостями запобігання загрозі $U_{km}(X_i) = \{0, \dots, 1\}$. Якщо захисні характеристики засобів задаються можливостями запобігання загрозі, то ймовірність реалізації загрози при впровадженому засобу захисту буде визначатися сумісною ймовірністю:

$$P_{km}(X_i) = P_{km} \cdot (1 - U_{km}(X_i)). \quad (7)$$

Далі фіксуємо вартість цього засобу S_{km} та розраховуємо показник (3). Цю процедуру виконуємо циклічно для всіх ресурсів *M* та всіх загроз *K*.

Після визначення комплекту засобів захисту для захисту всіх *M* ресурсів інформаційної системи розраховуємо інтегральний показник ефективності (5), далі розраховуємо вартість цього комплекту та порівнюємо з максимально допустимою вартістю S_{max}. Якщо умови (5) та (6) виконуються, то оптимізаційну задачу вважаємо виконаною.

Якщо умова (6) не виконується, то наступним кроком буде визначення менш критичних ресурсів інформаційної системи, для яких можна застосувати більш дешеви методи та засоби захисту. Наприклад, замість екранування приміщення або екранування засобів електронно-обчислювальної техніки застосовувати засоби активного електромагнітного маскування.

Застосування більш дешевих засобів захисту з множини $\vec{X} = \{X_1, X_2, \dots, X_B\}$, вимагає введення додаткового обмеження стосовно якості інформаційного захисту, а саме – ймовірність реалізації загрози при впроваджені більш дешевого засобу захисту $X_{j \in B}$ не повинна перевищувати допустиме значення:

$$P_{km}(X_{j \in B}) \leq P_{доп.} \quad (8)$$

Після заміни дорогого засобу захисту на більш дешевий знову розраховується інтегральний показник (5) та перевіряється умова (6). Ця процедура «здешевлення» КЗЗ виконується ітераційно до виконання умови (6) з урахуванням умови (8).

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 в інформаційній системі при обмеженому бюджеті компанії.

Література

1. Добринін І. С. Оптимізація вибору варіанту побудови системи захисту інформації від атак при антагоністичній грі / І. С. Добринін, М. П. Борова. *Системи озброєння і військова техніка*. 2018. № 2. С. 89 – 93. DOI: 10.30748/soivt.2018.54.12.

2. Пшеничних С. В. Математична модель оптимального вибору засобів захисту інформації при проектуванні комплексної системи захисту на об'єкті інформатизації / С. В. Пшеничних, І. С. Добринін, Д. Ю. Клочкова. *Проблеми телекомунікацій*. 2023. № 1(32). С. 45 – 58. DOI: 10.30837/pt.2023.1.04.

3. 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* [Текст]. Київ : Державна служба спеціального зв'язку України, 2007. 9 с.

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