УДК 621.396

О.К. Климович

Військовий інститут телекомунікацій та інформатизації
Національного технічного університету України «КПІ», Полтава

МЕТОДИЧНІ ОСНОВИ ОЦІНКИ ЗАХИЩЕНИХ АВТОМАТИЗОВАНИХ РОБОЧИХ МІСЦЬ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Дана робота присвячена розгляду методичних основ оцінки захищених автоматизованих робочих місць інформаційно-телекомунікаційної мережі військового призначення під час обробки електронної інформації. Наведена узагальнена характеристика основних груп методів оцінки захищених автоматизованих робочих місць. Запропоновано використання у якості базового експертного методу для вирішення поставленого завдання. При розгляді завдань подібного роду широко використовується метод аналізу ієрархій, який і необхідно застосувати для оцінки захищених автоматизованих робочих місць інформаційно-телекомунікаційної мережі військового призначення.

Ключові слова: *експертний метод, автоматизоване робоче місце, інформаційно-телекомунікаційна мережа.*

Вступ

В зв'язку з розвитком автоматизованих систем управління військового призначення удосконалення існуючої системи захисту інформаційних ресурсів повинно здійснюватися на підставі науково обґрунтованих критеріїв, виходячи із пріоритетних національних інтересів України, забезпечення її національної безпеки. Йде пошук доцільних шляхів створення і вдосконалення науково обґрунтованої, економічно доцільної системи захисту інформаційних ресурсів, спрямованої на те, щоб накопичені суспільством знання, наукові досягнення працювали передусім на розвиток економіки держави та забезпечення національної безпеки України [1].

При використанні засобів обчислювальної техніки і передачі даних з'являються нові проблеми збереження конфіденційності, цілісності і доступності інформації [2], що містить відомості, які становлять державну таємницю. Найбільш надійний захист інформації в автоматизованих системах і мережах різних класів можна забезпечити тільки за допомогою системного підходу. Він припускає, що рішення задачі повинне досягатися за рахунок використання сукупності організаційних і організаційно-технічних мір і заходів, а також криптографічних систем і засобів.

Виклад основного матеріалу

При постановці завдання оцінювання захищеності автоматизованого робочого місця як системи інформаційних ресурсів S необхідно визначити її наступні показники: вартість інформації, яка захищається, вірогідність злому, вартість самої системи захисту, продуктивність системи. За основний критерій захищеності використовується коефіцієнт захищеності K, що показує відносне зменшення ризику в захищеній системі в порівнянні з незахищеною системою [3]:

$$K = 1 - \frac{K_{зах}}{K_{наз}},$$

де $K_{зах}$ – ризик в захищеній системі; $K_{нез}$ – ризик в незахищеній системі.

Для завдання запропонованих параметрів оцінки захищеності системи можуть використовуватися різні групи методів, а саме статистичні методи, експертні методи, формальні методи, методи на основі критеріїв оцінки захищеності.

В основі статистичних методів лежить збирання та аналіз статистичних даних про події на протязі певного проміжку часу, що відбуваються в системі та впливають на її безпеку. Основним способом завдання інтенсивностей потоків загроз μ_i (вірогідностей загроз $p_i^з$) і вірогідностей зломів $p_i^{зл}$ є отримання цих значень на основі наявної статистики загроз безпеки системи, в якій реалізується відповідна підсистема захисту. Експертні методи ефективні при оцінці часткових показників захищеності, наприклад, при аналізі ризику, коли оцінюється ризик реалізації тієї або іншої загрози. В основі експертних методів лежить створення групи експертів для обговорення вразливих місць та загроз підсистеми захисту інформації у відповідній системі. Експерти під час загроз визначають рішення про ступінь її небезпеки для підсистеми захисту. Сутність формальних методів заключається в побудові на основі існуючих формальних апаратів моделі захищеної системи, якій характерна складна та різнорідна структура. У якості неформальних методів застосовують метод оцінки, що засновується на сукупності критеріїв захищеності. За допомогою використання методу критерії захищеності задаються вже на етапі розробки самої системи. Це характерно інформаційно-телекомунікаційній мережі військового призна-

чення, в якій програмно-апаратне забезпечення має спеціалізований характер.

Використання різних методів оцінки захищеності системи обумовлює вибір базового методу. З вищезазначених методів найбільш доцільним є використання експертних методів, тому що це пов'язано з їх ефективністю при оцінці часткових показників захищеності інформаційно-телекомунікаційної мережі військового застосування, наприклад, при аналізі збоїв в системі в зв'язку з впливом зовнішніх чи внутрішніх факторів, коли оцінюється ризик реалізації тієї або іншої загрози впливу чинника певного роду. Основою методів даного класу являються експертні системи, які повинні уміти пояснювати свою поведінку і свої рішення користувачу, так само, як це робить експерт-людина. Здібність до пояснення потрібна для того, щоб підвищити ступінь довіри користувача до порад системи, а також для того, щоб дати можливість користувачу знайти можливий дефект в міркуваннях системи. Це особливо необхідно в випадках, для яких характерна невизначеність, неточність інформації.

Існують наступні різновиди найбільш поширених експертних методів: метод ранжирування [4], метод попарних порівнянь [4, 5], метод Делфі [3], метод завдання вагових коефіцієнтів [6] і так далі.

Метод ранжування представляється у загальному вигляді так, що експерт або декілька експертів розташовують ознаки об'єкту або альтернативи в порядку переваги або у найбільш раціональному вигляді. Наприклад, перший об'єкт має найбільш важливу ознаку, другий являється наступним по важливості і так далі. У випадку коли дані від експертів зібрані, проводиться обробка отриманих оцінок. Визначається середній ранг і -ої ознаки об'єкту:

$$S_i = \frac{1}{n}\sum_{j=1}^{n} x_{ij},$$

де i – номер ознаки об'єкта; j – номер експерта; x_{ij} – ранг об'єкту.

Чим менше значення величини S_i, тим більша важливість цієї ознаки об'єкту. Для визначення збігу думок експертів розраховується коефіцієнт конкордації [5]. Кількісне значення коефіцієнту знаходиться в межах від 0 до 1, при цьому нуль означає повну протилежність думок експертів, а одиниця – повний збіг ранжирувань.

При досить великій кількості об'єктів або альтернатив використовується метод попарних порівнянь. Досить широке застосування набув метод аналізу ієрархій, що відноситься до класу методів попарних порівнянь. Досить складна проблема може бути представлена у вигляді трьохрівневої ієрархії (мета – критерії – альтернативи), а кожний з елементів ієрархії може при необхідності може бути представлений, в свою чергу, у вигляді трьохрівневої ієрархії і так далі. Під час застосування методу аналізу ієрархій встановлюються пріоритети критеріїв і оцінюється кожна з альтернатив за відповідними критеріями. У даному методі елементи одного рівня ієрархії порівняються попарно по відношенню до їхньої ваги на загальну для них характеристику. Система парних відомостей приводить до результату, що може бути представлений у вигляді симетричної матриці. Елементом матриці $a(i, j)$ є інтенсивність прояву елемента ієрархії i щодо елемента ієрархії j, яка оцінюється по шкалі інтенсивності від 1 до 9, що запропонована автором методу, де оцінки мають наступний сенс: 1 – рівна важливість; 3 – помірна перевага одного над іншим; 5 – істотна перевага одного над іншим; 7 – значна перевага одного над іншим; 9 – дуже сильна перевага одного над іншим; 2, 4, 6, 8 – відповідні проміжні значення. Якщо при порівнянні одного критерію i з іншим j отримано $a(i, j) = b$, то при порівнянні другого фактора з першим одержуємо $a(i, j) = 1/b$. Відносна сила, величина або ймовірність кожного окремого об'єкта в ієрархії визначається оцінкою відповідного йому елемента власного вектора матриці пріоритетів, що нормалізований до одиниці. Процедура визначення власних векторів матриць піддається наближенню за допомогою обчислення геометричної середньої. Локальні пріоритети перемножуються на пріоритет відповідного критерію на вищестоящому рівні й підсумуються по кожному фактору відповідно до критеріїв, на які впливає елемент.

Досить корисним побічним продуктом теорії є так званий індекс погодженості (ІП), що подає інформацію про ступінь порушення погодженості: $ІП = (\lambda_{max} - n)/(n-1)$. Разом з матрицею парних порівнянь ми маємо міру оцінки ступеня відхилення від погодженості. Якщо такі відхилення перевищують установлені межі, то тому, хто проводить судження, варто перевірити ще раз їх у матриці. Крім того, матриця попарних порівнянь відображає погоджені судження тоді, коли $\lambda_{max} = n$, тому $\lambda_{max} - n$ дає міру непогодженості та вказує на те, коли судження експертів необхідно перевірити. Якщо розділити індекс погодженості на число, що відповідає випадковій погодженості матриці того ж порядку, одержимо відношення погодженості, величина якого повинна бути порядку 10% або менш, щоб бути прийнятною. У деяких випадках допускається значення до 20%, але не більше, інакше треба перевірити свої судження.

Експертна оцінка початкових параметрів для розрахунку захищеності системи може здійснюватися з використанням методу Делфі [3], тобто групи експертів, яка створена з метою збирання інформації з певних джерел по визначеній проблемі. При цьому необхідно задати лінгвістичний словник можливих оцінок експертів, визначити набір питань і умовних значень

кваліфікацій окремих експертів. Після визначення всіх вхідних змінних проводиться почергове опитування кожного експерта. Після опитування всіх експертів з урахуванням їх кваліфікації визначається загальна оцінка групи й узгодженість (достовірність) відповідей для кожного питання. Експерт оцінює ефективність (вірогідність) відображення зломів елементами захисту $p_i^{зл}$ і вірогідність появи загроз $p_i^з$. Вірогідності експерт задає лінгвістичними оцінками, які за допомогою словника переводяться в числа $p_i^{зл}$ і $p_i^з$ в діапазоні $(0;1)$. Оцінка вірогідності появи загрози i-го вигляду в загальному потоці загроз задається в наступному вигляді [3]:

$$p_i^з = \frac{\mu_i}{\sum \mu_i}.$$

Враховуючи кваліфікацію експертів, розраховується їх вага (значущість) в групі:

$$\nu_e = \frac{k_e}{\sum k_e},$$

де k_e – кваліфікація експерта, що задається в деякому діапазоні залежно від досвіду, освіти і інших якостей експерта.

Потім оцінки підсумовуються з урахуванням ваг експертів:

$$p_i^{зл} = \sum p_{ie}^{зл} \cdot \nu_e ; \quad p_i^з = \sum p_{ie}^з \cdot \nu_e ,$$

де $p_{ie}^{зл}$ та $p_{ie}^з$ – оцінка вірогідностей відображення та появи загроз, виконані одним експертом; ν_e – «вага» експерта в групі.

Далі за допомогою середньоквадратичного відхилення розраховується узгодженість відповідей, яка може використовуватися для оцінки достовірності результатів. Максимальна узгодженість досягається при однакових значеннях оцінок експертів, мінімальна – при досить різних оцінках експертів.

Для визначення цільової функції при проектуванні підсистеми захисту інформації відповідної системи можливе використання ряду показників за допомогою методу завдання вагових коефіцієнтів [6]. Наприклад, для методу зваженої суми оцінок критеріїв корисність U багатокритеріального об'єкта задається залежністю [5, 6]:

$$U = \sum_{j=1}^{N} \omega_j q_j ,$$

де q_j – оцінка об'єкта по j-му критерію $(j = 1...N)$, яка вимірюється по кількісній шкалі, ω_j – вага (ваговий коефіцієнт) j-го критерію, що вимірюється також по кількісній шкалі. Мультиплікативний показник якості використовується шляхом перемножування часткових показників з врахуванням їхніх вагових коефіцієнтів. Корисність U багатокритеріального об'єкта задається залежністю [5, 6]:

$$U = \prod_{j=1}^{N} q_j^{\omega_j} ,$$

де q_j – оцінка об'єкта по j-му критерію $(j = 1...N)$, що вимірюється по кількісній шкалі; ω_j – вага (ваговий коефіцієнт) j-го критерію, що вимірюється також по кількісній шкалі. При використанні мінімаксного показника будемо вважати раціональною підсистему захисту інформації, яка забезпечує виконання умов [5, 6]:

$$U = f_p(q_1, ..., q_j, ..., q_m) = \underset{S_{СЗІ}}{\text{opt}} ;$$

$$q_j = q_j(S),\ j = \overline{1...N} ; \quad q_j \le q_{jN},\ j = \overline{1...N} ,$$

де q_{jN} – значення показника якості q_j, що є максимально допустимим, щодо вимог замовника до підсистеми захисту інформації. Під значеннями q_{1N}; q_{2N}; q_{3N}; q_{4N} уважаємо такі показники якості підсистеми захисту: q_{1N} – вартість інформації, що захищається; q_{2N} – вірогідність злому підсистеми захисту інформації; q_{3N} – вартість підсистеми захисту інформації; q_{4N} – продуктивність системи.

З множини варіантів побудови підсистеми захисту інформації даної системи необхідно вибрати раціональний варіант. Використання адитивного і мультиплікативного показників, можна зробити висновок про те, що перший з них базується на принципі справедливої абсолютної поступки за окремими показниками, а другий – на принципі справедливої відносної поступки, а мінімаксний показник забезпечує найкраще (найбільше) значення найгіршого (найменшого) з часткових показників якості.

Висновки

Отже дана узагальнена характеристика основних груп методів оцінки захищеності автоматизованого робочого місця інформаційно-телекомунікаційної мережі військового призначення. На основі проведеного аналізу в якості базового методу запропоновано використання експертного методу, в основі якого фігурує група, створена з метою збирання інформації з певних джерел по визначеному завданню оцінки захищеності відповідної системи.

Методика оцінки захищених автоматизованих робочих місць телекомунікаційних мереж військового призначення припускає рішення завдання багатокритеріального вибору при наявності різнорідних критеріїв. Якісне рішення даного завдання неможливо без використання систем підтримки прийняття рішення, які базуються на одному з методів аналітичного планування. Для рішення завдань подібного роду в аналітичному плануванні широко застосовується метод аналізу ієрархій, який і необхідно застосувати для оцінки захищених автоматизованих робочих місць телекомунікаційних мереж військового призначення.

Список літератури

1. Мастяниця Й.У. Захист інформаційних ресурсів України: проблеми і шляхи їх розв'язання / Й.У. Мастяниця, О.В. Соснін, Л.Є. Шиманський // Національний інститут стратегічних досліджень. – К., 2000.

2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебн. для вузов / В.Г. Олифер, Н.А. Олифер. 4-е изд. – СПб.: Питер, 2010. – 944 с.

3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. – Санкт-Петербург: Видавництво «Наука и Техника», 2004. – 384 с.

4. Самохвалов Ю.Я. Экспертное оценивание. Методический аспект / Ю.Я. Самохвалов, Є.М. Науменко. – К.: Видавництво ДУІКТ, 2007. – 263 с.

5. Інтелектуальні системи підтримки прийняття рішень: Теорія, синтез, ефективність / В.О. Тарасов, Б.М. Герасимов, І.О. Левін, В.О. Корнійчук. – К.: МАКНС, 2007. – 336 с.

6. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – 2001. – 608 с.

Надійшла до редколегії 4.06.2012

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних сил ім. І. Кожедуба. Харків.

МЕТОДИЧЕСКИЕ ОСНОВЫ ОЦЕНКИ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ВОЕННОГО НАЗНАЧЕНИЯ

О.К. Климович

Данная работа посвящена рассмотрению методических основ оценки защищенных автоматизированных рабочих мест информационно-телекоммуникационной сети военного назначения во время обработки электронной информации. Приведена обобщенная характеристика основных групп методов оценки защищенных автоматизированных рабочих мест. Предложено использование в качестве базового экспертного метода для решения поставленного задания. При рассмотрении заданий подобного рода широко используется метод анализа иерархий, который и необходимо применить для оценки защищенных автоматизированных рабочих мест информационно-телекоммуникационной сети военного назначения.

Ключевые слова: *экспертный метод, автоматизированное рабочее место, информационно-телекоммуникационная сеть.*

METHODICAL BASES OF ESTIMATION OF THE PROTECTED WORKSTATIONS OF INFORMATIVELY-TELECOMMUNICATION NETWORK OF MILITARY SETTING

O.K. Klimovich

This work is devoted to consideration of methodical bases of estimation of the protected workstations of informatively-telecommunication network of the military setting during treatment of electronic information. Resulted generalized description of basic groups of methods of estimation of the protected workstations. The use is offered in quality of base expert method for the decision of the put task. At consideration of tasks of a similar family the method of analysis of hierarchies, which it is necessary to apply for estimation of the protected workstations of informatively-telecommunication network of the military setting, is widely used.

Keywords: *expert method, workstation, informatively-telecommunication network.*