УДК 621.396 DOI: 10.30748/soivt.2018.53.20

О.К. Климович

Національна академія сухопутних військ ім. гетьмана Петра Сагайдачного, Львів

МЕТОДИЧНІ ОСНОВИ ОЦІНКИ КОНТРОЛЮ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Під час проведення антитерористичної операції йде пошук доцільних шляхів створення і вдосконалення науково обґрунтованої, економічно доцільної системи захисту інформаційних ресурсів в інформаційно-телекомунікаційних мережах спеціального призначення. Дана робота присвячена розгляду методичних основ оцінки контролю захищеності інформаційно-телекомунікаційних мереж спеціального призначення. Метою статті є підвищення захищеності інформаційно-телекомунікаційних мереж спеціального призначення за рахунок використання у якості базового методу аналізу ієрархій та апарату нейро-нечітких мереж для оцінки захищеності мереж даного класу. Наведена узагальнена характеристика основних груп методів оцінки контролю захищеності інформаційно-телекомунікаційних мереж даного класу. При постановці завдання оцінки контролю захищеності інформаційно-телекомунікаційних мереж спеціального призначення як системи інформаційних ресурсів визначаються її наступні показники: пріоритетність інформації, яка захищається, вірогідність злому, вартість системи захисту, продуктивність системи. Для завдання запропонованих параметрів оцінки захищеності системи можуть використовуватися методи дослідження, які включають теорії: графів, систем підтримки прийняття рішень, нечітких множин, нейронних мереж, методи багатокритеріальної оптимізації, експертні методи. Запропоновано використання у якості базового методу аналізу ієрархій та апарату нейро-нечітких мереж для подальшої розробки методу оцінки контролю захищеності інформаційно-телекомунікаційної мережі спеціального призначення.

Ключові слова: *метод аналізу ієрархій, теорія нечітких множин, теорія нейронних мереж, інформаційно-телекомунікаційна мережа спеціального призначення.*

Вступ

В зв'язку зі стрімким розвитком інформаційно-телекомунікаційних мереж удосконалення існуючої системи захисту інформаційних ресурсів повинно здійснюватися на підставі використання науково обґрунтованих критеріїв, сучасних протоколів передачі інформації, виходячи із пріоритетних національних інтересів, забезпечення національної безпеки держави [1–10]. Під час проведення антитерористичної операції 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 забезпечення національної безпеки та оборони України. **Метою статті** є підвищення захищеності інформаційно-телекомунікаційних мереж спеціального призначення за рахунок використання у якості базового методу аналізу ієрархій та апарату нейро-нечітких мереж для оцінки захищеності мереж даного класу.

Основна частина

При постановці завдання оцінки контролю захищеності інформаційно-телекомунікаційних мереж спеціального призначення як системи інформаційних ресурсів S необхідно визначити її наступні показники: пріоритетність інформації, яка захищається, вірогідність злому, вартість самої системи захисту, продуктивність системи [3]. Для завдання запропонованих параметрів оцінки захищеності системи можуть використовуватися методи дослідження, які включають теорії: графів, систем підтримки прийняття рішень, нечітких множин, нейронних мереж, методи багатокритеріальної оптимізації, експертні методи [11–14].

Абстрактний орієнтований граф є основою планування дій людини-оператора, зміни порядку послідовності його дій, проведення операцій. Постановка завдань мережевого планування починається з виявлення вузлових моментів (подій) операції, що визначають початок і кінець основних її етапів, після якого визначаються заходи, що приводять до здійснення кожної події й супроводжувані витратами часу й ресурсів. Потім події й відповідні їм роботи вибудовуються в деяку логічну послідовність, що представляється графічно у вигляді мережевого графа, які відображають всі шляхи досягнення кінцевої мети операції. Побудова мережевого графа починається з визначення переліку подій і їхнім нанесенням на граф відповідно до рангу. Ранг події визначається його порядковим номером у загальній послідовності подій, так, наприклад, вихідна подія має нульовий ранг, що випливає за ним – перший і т.д. Потім на граф наносяться роботи у вигляді ліній, що з'єднують вихідні й наступні події. У загальному випадку мережевий граф (рис. 1) представляє собою граф, вузли якого a_x – події, а орієнтовані дуги A_{xy} – роботи, $x \le y$. При цьому в графі будь-яка дуга відображає тільки одну роботу, а у випадку виникнення ситуації, коли дві роботи мають ті самі вихідні й вхідні вузли (події) уводять додаткову фіктивну роботу, не пов'язану з витратами часу й інших ресурсів.

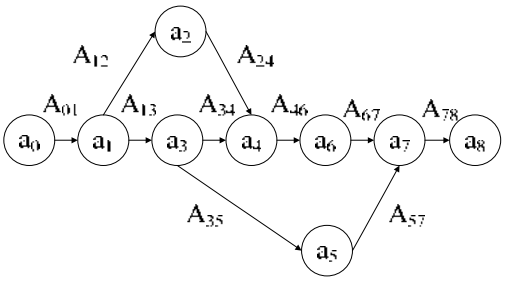

Рис. 1. Мережевий граф

Одна з можливих послідовностей подій і робіт від вихідної події до завершальної являє собою шлях мережевого графа, а шлях, що має максимальний час виконання кожної із вхідних у нього робіт і сумарний час виконання всієї операції є критичним шляхом. 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 спеціального призначення. Існують такі різновиди найбільш поширених експертних методів: метод ранжирування, метод попарних порівнянь, метод Делфі, метод завдання вагових коефіцієнтів і так далі [11–14].

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 k-ої ознаки об'єкту:

$$R_k = \left(\sum_{l=1}^{n} z_{kl}\right) \Big/ n ,$$

де k – номер ознаки об'єкта; l – номер експерта; z_{kl} – ранг об'єкту. Чим менше значення величини R_k, тим більша важливість цієї ознаки об'єкту. Для визначення збігу думок експертів розраховується коефіцієнт конкордації. 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 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 b(k,l) є інтенсивність прояву елемента ієрархії k щодо елемента ієрархії l , 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 k з іншим l отримано b(k,l)=c, то при порівнянні другого фактора з першим одержуємо b(k,l)=1/c. 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.

Формальним апаратом для обробки експертної інформації є математичний апарат нечітких множин, що дозволяє формувати правила прийняття рішень по оцінці контролю захищеності вузлів мережі. Формалізувати відповідну інформацію можливо, використовуючи лінгвістичні змінні «пріоритетність інформації», «вірогідність злому», «вартість системи захищеності», «продуктивність системи». Лінгвістичні змінні «пріоритетність інформації», «вірогідність злому», «вартість системи захищеності» являються вхідними змінними, лінгвістична змінна «продуктивність системи» – вихідна змінна. Будуються функції приналежності для кожної лінгвістичної змінної, формується нечітка база знань на основі продукційних правил, що обумовлюється необхідністю обліку реального масштабу часу і зручності подання інформації про процедури та умови їх виконання. Отже рішення завдання визначення порядку контролю захищеності вузлів мережі базується на використанні апарату теорії нечітких множин [12]. В подальшому результат оцінки контролю захищеності відповідної мережі може бути використаний із застосуванням теорії нейронних мереж. Сутність нейронної мережі полягає у наближенні функцій багатьох змінних за допомогою лінійних операцій. На вхід мережі подається набір значень і паралельно задається відповідний набір вихідних значень (рис. 2) [11]. Нейронні мережі і нечітка логіка являються універсальними апроксимаціями складних (нелінійних) функціональних залежностей в багатьох інтелектуальних задачах кібернетики. Головною особливістю нейронних мереж є їх здібність до навчання, яка реалізується за допомогою спеціально розроблених алгоритмів. Для навчання нейронної мережі не вимагається ніякої апріорної інформації про структу-

ру шуканої функціональної залежності. Потрібна лише повчальна вибірка у вигляді експериментальних пар «входи-виходи». Перевагою нечіткої логіки є можливість використання експертних знань про структуру об'єкту у вигляді лінгвістичних висловів: якщо «входи», то «вихід». Проте апарат нечіткої логіки не містить механізмів навчання, тому результати нечіткого логічного висновку сильно залежать від виду функцій приналежності, якими формалізуються нечіткі терми. Одержувана в результаті об'єднання нечіткої логіки з нейронними мережами нейронечітка мережа володіє двома найважливішими інтелектуальними властивостями: лінгвістичністю, тобто використанням знань на природній мові, і здатністю до навчання в реальному масштабі часу [11].

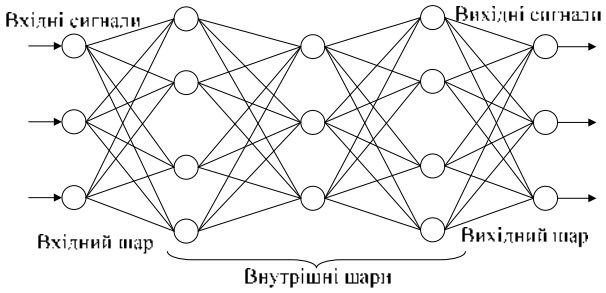

Рис. 2. Структура нейронної мережі

Аналіз літератури [14] показав, що всі численні методи розв'язання багатокритеріальних задач можливо звести до трьох груп методів: методу головного показника, методу результуючого показника, лексикографічного методу (методу послідовних поступок).

Метод головного показника заснований на переведенні всіх показників якості, окрім якого-небудь головного, в розряд обмежень типу рівностей або нерівностей. Присвоюємо головному показнику номер $q_1(S)$. Тоді задача зводиться до однокритеріної задачі вибору системи $S \in M_S$, яка володіє мінімальним значенням показника $q_1(S)$ при наявності обмежень типу рівностей та нерівностей, тобто має вигляд $\min\limits_{S \in M_S} q_1(S)$ при обмеженнях $q_1(S) = q_{j0}$; $j = 2, \ldots, v$; $q_w(S) \le q_{w0}$; $w = v+1, \ldots, d$; $q_h(S) \ge q_{h0}$; $h = d+1, \ldots, m$.

У більшості випадків немає достатніх підстав для того, щоб рахувати який-небудь визначений один показник головним, а всі інші – другорядними. В той же час для показників якості $q_2(S), \ldots, q_m(S)$, які переводяться в розряд обмежень, достатньо важко встановити їх допустимі значення. Метод результуючого показника якості заснований на формуванні узагальненого показника шляхом інтуїтивних оцінок впливу часткових показників якості $q_1, \ldots, q_m$ на результуючу якість виконання системою її функцій. Оцінки такого впливу даються групою фахівців – експертів, які мають досвід розробки подібних систем.

Найбільше застосування серед результуючих показників якості отримали адитивний, мультиплікативний та мінімаксний показники.

Для визначення цільової функції при проектуванні підсистеми контролю захищеності інформації відповідної системи можливе використання ряду показників за допомогою методу завдання вагових коефіцієнтів. Наприклад, для методу зваженої суми оцінок критеріїв корисність U_α багатокритеріального об'єкта задається залежністю [14]:

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

де q_j – оцінка об'єкта по j-му критерію $(j = 1...M)$, 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_β багатокритеріального об'єкта задається залежністю [14]:

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

де q_j та ω_j мають той же сенс, що і в адитивному показнику.

У випадках, коли вигляд результуючої цільової функції достатньо складно обґрунтувати або застосувати, використовують мінімаксний показник. Правило вибору оптимальної системи *S* має такий вигляд [14]:

коли вагові коефіцієнти часткових показників відсутні

$$\max_{S \in M,\ 1 \le j \le m} \min \left\{ q_1(S), \ldots, q_j(S), \ldots, q_m(S) \right\};$$

коли вагові коефіцієнти визначені

$$\max_{S \in M,\ 1 \le j \le m} \min \left\{ q_1^{\omega_1}(S), \ldots, q_j^{\omega_j}(S), \ldots, q_m^{\omega_m}(S) \right\}.$$

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.

При використанні лексикографічного методу для визначення цільової функції при проектуванні підсистеми контролю захищеності інформації показники якості q_j впорядковані за важливістю $q_1(S) > q_2(S) > \ldots > q_m(S)$. Суть лексикографічного методу полягає у виділенні спочатку множини альтернатив з найкращою оцінкою по найбільш важливому показнику. Якщо альтернатива єдина, то вона вважається найкращою; якщо їх декілька, то з них виділяються ті, які мають кращу оцінку по другому показнику й т.д. Для розширення множини розглянутих альтернатив і поліпшення якості рішення по сукупності показників може призначатися поступка, у межах

якої альтернативи вважаються еквівалентними. Принциповою особливістю розглянутої задачі вибору раціонального варіанта підсистеми захисту інформації являється переважно якісний характер показників, які трактуються як вимоги, що задаються до підсистеми захисту інформації. В зв'язку з цим розглянуті методи багатокритеріальної оптимізації повинні формулюватися в нечіткій постановці. Як в класичній так і в нечіткій постановці вибір методу рішення багатокритеріальної задачі визначається тим, в якому вигляді представлена експертна інформація про перевагу показників або їх важливості. В подальшому під значеннями q_1; q_2; q_3; q_4 вважаємо такі показники якості підсистеми захисту: q_1 – приорітетність інформації; q_2 – вірогідність злому підсистеми; q_3 – вартість підсистеми; q_4 – продуктивність підсистеми.

Висновки

Отже дана узагальнена характеристика основних груп методів оцінки контролю захищеності інформаційно-телекомунікаційних мереж спеціального призначення. Якісне рішення даного завдання неможливе без використання систем підтримки прийняття рішення. На основі проведеного аналізу в якості базового запропоновано використання методу аналізу ієрархій та апарату нейронно-нечітких мереж по визначенню завдання оцінки контролю захищеності відповідної системи. Наступним етапом дослідження буде розробка методу оцінки захищеності інформаційно-телекомунікаційних мереж спеціального призначення.

Список літератури

1. Дружинін С.В. Визначення факторів та параметрів процесу функціонування інформаційно-телекомунікаційної мережі ЗС України / С.В. Дружинін, О.К. Климович // Зб. наук. праць ВА. – Одеса: ВА, 2017. – Вип. 2 (8). – С. 171-177.

2. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах / О.Г. Пузиренко, С.О. Івко, О.О. Лаврут, О.К. Климович // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 3 (128). – С. 75-79.

3. Климович О.К. Методичні основи оцінки захищених автоматизованих робочих місць інформаційно-телекомунікаційної мережі військового призначення / О.К. Климович // Збірник наукових праць Харківського університету Повітряних Сил імені Івана Кожедуба. – Х.: ХУПС, 2012. – Вип. 3 (32). – С. 115-118.

4. Meier S. Efficient Construction of Machine-Checked Symbolic Protocol Security Proofs / S. Meier, C. Cremers, D. Basin // Journal of Computer Security. – 2013. – Vol. 21, No. 1. – P. 41-87.

5. Fan Y. Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks / Y. Fan, Y. Jiang, H. Zhu, J. Chen, X. Shen // IEEE Trans. on Wireless Communication. – 2011. – Volume 1. – No. 3. – P. 834-843.

6. Singh Y. Information Theory test based Performance Evaluation of Cryptographic Techniques / Y. Singh, Y. Chaba // International Journal of Information Technology and Knowledge Management. – 2008. – Volume 1. – No. 2. – P. 475-483.

7. Zhang P. ANOC: Anonymous Network-Coding Based Communication with Efficient Cooperation / P. Zhang, Y. Jiang, C. Lin, P. Lee, J. Lui // IEEE Journal on Selected Areas in Communications. – 2012. – Vol. 30, No. 9. – P. 1738-1745.

8. Sharma R. Analysis of Security Protocols in Wireless Sensor Networks / R. Sharma, Y. Chaba, Y. Singh // International Journal of Advanced Networking Applications. – 2010. – Vol. 2. – Issue 3. – P. 707-713.

9. Cai N. Secure Network Coding on a Wiretap Network / N. Cai, R.W. Yeung // IEEE Transactions on Information Theory. – 2011. – Vol. 57, No. 1. – P. 424-435.

10. Ahlswede R. Network information flow / R. Ahlswede, N. Cai, S.R. Li, R.W. Yeung // IEEE Transactions on Information Theory. – 2000. – Vol. 47, No. 7. – P. 1204-1216.

11. Барский А.Б. Нейросетевые методы оптимизации решений / А.Б. Барский. – СПб.: Интермедия, 2016. – 312 с.

12. Зайченко Ю.П. Нечеткие модели и методы в интеллектуальных системах / Ю.П. Зайченко. – К.: Издательский дом "Слово", 2008. – 344 с.

13. Субботін С.О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень: Навчальний посібник / С.О. Субботін – Запоріжжя: Запорізький національний технічний університет, 2008. – 341 с.

14. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К.: ДиаСофт, 2002. – 688 с.

References

1. Druzhynin, S.V. and Klimovich, O.K. (2017), "Vyznachennia faktoriv ta parametriv protsesu funktsionuvannia informatsiino-telekomunikatsiinoi merezhi Zbroinykh Syl Ukrainy" [Definition of factors and parameters of the process of functioning of the information and telecommunication network of the Armed Forces of Ukraine], *Collection of scientific works of the Military Academy*, No. 2(8), pp. 171-177.

2. Puzyrenko O.H., Ivko S.O., Lavrut O.O. and Klymovych O.K. (2015), "Zastosuvannia modelei otsiniuvannia ryzykiv informatsiinoi bezpeky v informatsiino-telekomunikatsiinykh systemakh" [Application of information security risk assessment models in information and telecommunication systems], *Information Processing Systems*, No. 3(128), pp. 75-79.

3. Klimovich, O.K. (2012), "Metodychni osnovy otsinky zakhyshchenykh avtomatyzovanykh robochykh mists informatsiino-telekomunikatsiinoi merezhi viiskovoho pryznachennia" [Methodical bases of estimation of workstations protected information and telecommunication networks], *Scientific Works of Kharkiv National Air Force University*, No. 3(32), pp. 115-118.

4. Meier, S., Cremers, C. and Basin D. (2013), "Efficient Construction of Machine-Checked Symbolic Protocol Security Proofs", *Journal of Computer Security*, Vol. 21, No. 1, pp. 41-87.

5. Fan, Y., Jiang, Y., Zhu, H., Chen, J. and Shen, X. (2011), "Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks", *IEEE Transactions on Wireless Communication*, Vol. 1, No. 3, pp. 834-843.

6. Singh, Y. and Chaba, Y. (2008), "Information Theory test based Performance Evaluation of Cryptographic Techniques", *International Journal of Information Technology and Knowledge Management*, Vol. 1, No. 2, pp. 475-483.

7. Zhang, P., Jiang, Y., Lin, C., Lee, P. and Lui J. (2012), "ANOC: Anonymous Network-Coding Based Communication with Efficient Cooperation", *IEEE Journal on Selected Areas in Communications*, Vol. 30, No. 9, pp. 1738-1745.

8. Sharma, R., Chaba, Y. and Singh Y. (2010), "Analysis of Security Protocols in Wireless Sensor Networks", *International Journal of Advanced Networking Applications*, Vol. 2, Issue 3, pp. 707-713.

9. Cai, N. and Yeung, R.W. (2011), "Secure Network Coding on a Wiretap Network", *IEEE Transactions on Information Theory, Vol. 57*, No. 1, pp. 424-435.

10. Ahlswede, R., Cai, N., Li, S.R. and Yeung, R.W. (2000), "Network information flow", *IEEE Transactions on Information Theory*, Vol. 47, No. 7, pp. 1204-1216.

11. Barskyi, A.B. (2016), "*Neirosetevye metodu optymyzatsyy reshenyi*" [*Neural network solutions optimization methods*], Yntermedyia, Sankt-Peterburh, 312 p.

12. Zaichenko, Yu.P. (2008), "*Nechetkye modely y metodы v yntellektualnыkh systemakh*" [*Fuzzy models and methods in intelligent systems*], Yzdatelskyi dom "Slovo", Kyiv, 344 p.

13. Subbotin, S.O. (2008), "*Podannia y obrobka znan u systemakh shtuchnoho intelektu ta pidtrymky pryiniattia rishen: Navchalnyi posibnyk*" [*Presentation and processing of knowledge in systems of artificial intelligence and decision support: A manual*], Zaporizkyi natsionalnyi tekhnichnyi universytet, Zaporizhzhia, 341 p.

14. Domarev, V.V. (2002), "*Bezopasnost ynformatsyonnukh tekhnolohyi. Metodolohyia sozdanyia system zashchytu*" [*Security of information technology. Methodology for creating protection systems*], DyaSoft, Kyiv, 688 p.

Надійшла до редколегії 10.01.2018
Схвалена до друку 20.02.2018

Відомості про автора:
Климович Олег Костянтинович
кандидат технічних наук старший науковий співробітник
докторант Національної академії сухопутних військ
ім. гетьмана П. Сагайдачного,
Львів, Україна
orcid.org/0000-0003-3863-4984
e-mail: vanpersi1950@gmail.com

Information about the author:
Oleg Klimovich
Candidate of Sciences Senior Research
Doctoral student of of Hetman Petro Sahaidachnyi
National Army Academy
Lviv, Ukraine
orcid.org/0000-0003-3863-4984
e-mail: vanpersi1950@gmail.com

МЕТОДИЧЕСКИЕ ОСНОВЫ ОЦЕНКИ КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

О.К. Климович

Во время проведения антитеррористической операции идет поиск подходящих путей создания и совершенствования научно обоснованной, экономически целесообразной системы защиты информационных ресурсов в информационно-телекоммуникационных сетях специального назначения. Данная работа посвящена рассмотрению методических основ оценки контроля защищенности информационно-телекоммуникационных сетей специального назначения. Целью статьи является повышение защищенности информационно-телекоммуникационных сетей специального назначения за счет использования в качестве базового метода анализа иерархий и аппарата нейро-нечетких сетей для оценки защищенности сетей данного класса. Приведена обобщенная характеристика основных групп методов оценки контроля защищенности информационно-телекоммуникационных сетей данного класса. При постановке задачи оценки контроля защищенности информационно-телекоммуникационных сетей специального назначения как системы информационных ресурсов определяются ее следующие показатели: приоритетность информации, которая защищается, вероятность взлома, стоимость системы защиты, продуктивность системы. Для задания предложенных параметров оценки защищенности системы могут использоваться методы исследования, включающие теории: графов, систем поддержки принятия решений, нечетких множеств, нейронных сетей, методы многокритериальной оптимизации, экспертные методы. Предложено использование в качестве базового метода анализа иерархий и аппарата нейро-нечетких сетей для дальнейшей разработки метода оценки контроля защищенности информационно-телекоммуникационной сети специального назначения.

Ключевые слова: *метод анализа иерархий, теория нечетких множеств, теория нейронных сетей, информационно-телекоммуникационная сеть специального назначения.*

METHODOLOGICAL BASES OF ESTIMATION OF SECURITY CONTROL OF THE INFORMATION AND TELECOMMUNICATION NETWORK OF SPECIAL PURPOSE

O. Klimovich

During the antiterrorist operation, there is a search for suitable ways to create and improve a science-based, economically feasible system of protecting information resources in information and telecommunications networks for special purposes. This work is devoted to the consideration of the methodological basis for assessing the monitoring of the protection of information and telecommunications networks for special purposes. The purpose of the article is to increase the security of information and telecommunication networks for special purposes by using as a basic method of analyzing hierarchies and the apparatus of neural-fuzzy networks to assess the security of networks of this class. A generalized characteristic of the main groups of methods for assessing the control over the security of information and telecommunication networks of this class is given. When setting the task of assessing the security monitoring of information and telecommunications networks of a special purpose as a system of information resources, its following indicators are determined: the priority of information that is protected, the probability of hacking, the cost of the protection system, the productivity of the system. To specify the proposed parameters for assessing the security of the system, research methods can be used that include theories: graphs, decision support systems, fuzzy sets, neural networks, multi-criteria optimization methods, expert methods. The use of the hierarchy analysis and the apparatus of neural-fuzzy networks as a basic method for the further development of the method for assessing the control of the security of information-telecommunication network of special purpose.

Keywords: *method of analysis of hierarchies, theory of fuzzy sets, theory of neural networks, information and telecommunications network of special purpose.*