УДК 004.621.3
DOI https://doi.org/10.32782/2663-5941/2022.6/09

Розорінов Г.М.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Сірченко І.А.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ЕКСПЕРТНА ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ РОЗПОВСЮДЖЕННЯ АУДІОВІЗУАЛЬНОГО КОНТЕНТУ

Пропонується методика і тести для експертної економічної оцінки ефективності застосування систем захисту інформації в мережах розповсюдження аудіовізуального контенту.

Показано, що при економічній оцінці системи крім витрат на неї необхідно також враховувати взаємодію між підсистемами, що входять в її склад (рівні захисту, рубежі захисту і таке інше).

Відповідно до цієї методики необхідно відповісти на сім груп питань, на підставі яких експертна система ухвалює рішення про доцільність прийняття системи захисту інформації. Аналіз вимог до системи захисту інформації проводиться відповідно до аналізу спрямованості її діяльності, функціями і процедурами захисту інформації на об'єкті.

Проте при аналізі цих питань виникають такі основні проблеми: контроль доступу до вразливої і секретної інформації; профілі секретності доступу: забезпечення і створення свідомого відношення до секретності в організації, розробка документації, що визначає політику відносно секретності на підставі нормативних документів, При цьому необхідно враховувати специфічні труднощі й в першу чергу до них слід віднести розподіл пріоритетів для інформації, що вимагає захисту, шляхом визначення відносної уразливості і секретності інформації. Крім цього, до основних проблем, які виникають при отриманні відповідей на поставлені питання, можна віднести зміни в технології захисту, які можуть бути використані як зловмисниками, так і захисниками інформації, а також встановити вимоги до фінансування заходів по захисту інформації.

Складнощі, які виникають при вирішенні цих питань зв'язані також з необхідністю уникнення конфліктів із-за ресурсів, розробки планів реалізації і запобігання конфліктам при розвитку системи захисту.

Аналіз відповідей на поставлені питання показує, що вони не мають чіткої межі. На питання можна дати декілька однотипних відповідей, що може привести до неякісної оцінки. Суворі правила, закладені в експертні системи, не дають оптимального рішення.

Прийнявши припущення, що відповідь несе в собі деяку нечіткість, зроблено висновок, що для експертної системи необхідно використовувати апарат нечіткої логіки. Тоді відповідно до отриманих відповідей, використовуючи апарат нечіткої логіки, експертна система ухвалює оптимальне і обгрунтоване рішення.

Використовуючи нечітку множину, визначається узагальнена відносна відстань Хеммінга, потім – індекс нечіткості, по якому видається експертна оцінка.

Ключові слова: *захист інформації, мережа, нечітка множина, оцінка ефективності.*

Постановка проблеми. В даний час найчастіше застосовуються економічні критерії для оцінки ефективності застосування систем захисту інформації (СЗІ) в мережах розповсюдження аудіовізуального контенту (МР АВК) [1, 2].

Як критерії економічності наводяться приведені витрати і обчислювана на їх основі економія витрат. Такі критерії не мають яких-небудь принципових переваг, за винятком фактору зручності застосування. Разом з цими критеріями отримав поширення і так званий критерій повних витрат [3–5]. При використанні цього критерію і параметрів: $C_к$ – одноразові капітальні витрати, що мають місце у момент встановлення системи захисту; $C_р$ – експлуатаційні витрати в одиницю часу; $E_Т$ – позитивний ефект в одиницю часу, отриманий від впровадження системи захисту, – ефективність системи захисту оцінюється таким чином:

$$T_o = \frac{C_к}{E_T - C_p} \text{ – термін окупності,} \quad (1)$$

$$C_{пр} = C_к + O_н C_p \text{ – приведені витрати,} \quad (2)$$

де $O_н$ – нормативний термін окупності;

$$C = C_к + T_c C_p \text{ – повні витрати,} \quad (3)$$

де T_c – термін служби або передбачуваний термін використання системи захисту.

Витрати по виразах (2) і (3) є функціями часу, а відмінність між приведеними і повними витратами полягає в тому. що перші обчислюються за час, який дорівнює нормативному терміну окупності, а другі – за повний час використання системи захисту.

Окрім відмічених вище критеріїв, при економічній оцінці системи крім витрат на неї необхідно також враховувати взаємодію між підсистемами, що входять в її склад (рівні захисту, рубежі захисту і таке інше) [6, 7].

Тому можна припустити, що повна вартість системи захисту інформації буде сумою вартостей її підсистем:

$$C_п = \sum_{i=1}^{i=n} C_i \,. \quad (4)$$

Також при економічній оцінці СЗІ необхідно враховувати в якій категорії систем з обмеженим доступом зберігається, обробляється і функціонує об'єкт захисту, а також до якої категорії відноситься сам об'єкт.

Метою роботи є експертна економічна оцінка ефективності застосування систем захисту інформації в мережах розповсюдження аудіовізуального контенту.

Виклад основного матеріалу. Найбільш поширеними в даний час є дві методики економічної оцінки СЗІ [8].

Забезпечення необхідного рівня захисту $P_з$ при мінімальних витратах $C_{мін}$:

$$\begin{cases} C_{мін} \to \min \\ P \ge P_з \end{cases}. \quad (5)$$

Забезпечення максимального рівня захисту при обмежених витратах C_o:

$$\begin{cases} P \to \max \\ C_o \le C \end{cases}. \quad (6)$$

На підставі цього проведемо оцінку економічної доцільності побудови системи захисту інформації.

Одразу встановимо, що $C_o \le kQ$, де Q – величина, що характеризує витрати із-за просочування інформації або несанкціонованих дій зловмисників (розмірність така ж, як $P_з$; k – статистичний коефіцієнт, який враховує витрати на СЗІ).

Відповідно до [5, 8] k знаходиться у діапазоні значень 0,05…0,20. Отже, співвідношення між C_o і Q, коли C_o в системі захисту інформації відповідає від 5 до 20% величини збитку, що обумовлений просочуванням інформації, вважаються за оптимальні. Інколи вважають, що витрати на систему захисту інформації повинні складати 20–30% від вартості інформаційної системи і локальної мережі об'єкту в цілому. Якщо вказані витрати менше 5%, тоді є ризик несанкціонованого отримання інформації зловмисником, якщо ж витрати перевищують 20%, тоді доцільно переглянути заплановані заходи і структуру системи захисту інформації.

Для точнішої і об'єктивнішої економічної оцінки ефективності системи захисту інформації в роботі пропонується комп'ютерна експертна методика і тести.

Відповідно до цієї методики необхідно відповісти на сім груп питань, на підставі яких експертна система ухвалює рішення про доцільність прийняття системи захисту інформації. Аналіз вимог до системи захисту інформації проводиться відповідно до аналізу спрямованості її діяльності, функціями і процедурами захисту інформації на об'єкті.

Відповідно до ***першої*** групи визначається інформація, що підлягає захисту. При цьому необхідно виділити інформацію, яку необхідно захистити від небажаної дії або не допускати її витоку. Аналізуючи наочну область в процесі пошуку рішення необхідно відповісти на такі питання:

– Які дані можуть збиратися?

– Хто може цікавитися цими даними?

– Чому вони цікавляться ними?

– Коли ці дані потрібні?

– Чи проходять через мережу об'єкту нові дані та нові користувачі даних?

– Які принципи використовуються для оцінки цінності інформації?

– Яка законодавча і соціальна відповідальність?

– Який захист необхідний для інформації кожного виду?

У ***другій*** групі питань здійснюється з'ясування можливих каналів просочування інформації. При цьому аналізується:

– Які конкретні співробітники мають доступ до конфіденційних даних?

– Хто повинен змінити інформацію, чому, коли?

– Чи проходили ці співробітники перевірку?

– Чи організуються й реалізуються в повному обсязі комп'ютерні заходи?

– Чи добре документуються і реалізуються комп'ютерні заходи?

– Чи є програми навчання, підготовки і перепідготовки персоналу?

Проте при аналізі цих питань виникають такі основні проблеми: контроль доступу до вразливої і секретної інформації; профілі секретності доступу: забезпечення і створення свідомого відношення до секретності в організації, розробка документації, що визначає політику відносно секретності на підставі нормативних документів, та ін.

Третя група питань це – оцінка уразливості й ризику. На цьому етапі оцінюється:

– Які специфічно вразливі точки має об'єкт, що треба оцінити?

– Наскільки може бути зменшений ризик при заданому збільшенні об'єму заходів захисту інформації?

При цьому необхідно враховувати проблеми і в першу чергу до них слід віднести розподіл пріоритетів для інформації, що вимагає захисту, шляхом визначення відносної уразливості і секретності інформації.

До ***четвертої*** групи питань відноситься визначення вимог до системи захисту інформації. Потрібно сформулювати і оцінити необхідний рівень захисту і на підставі цього визначити основні економічні характеристики системи захисту. При цьому необхідно відповісти на такі питання:

– Які технічні заходи безпеки використовуються?

– Яка вартість технічних заходів захисту?

– Наскільки ефективні доступні заходи захисту?

– Наскільки уразливі елементи системи захисту інформації?

– Який ризик (аналіз і прогнозування можливих наслідків, які можуть, викликати ці проблеми)?

До основних проблем, які виникають при отриманні відповідей на ці питання, можна віднести зміни в технології захисту, які можуть бути використані як зловмисниками, так і захисниками інформації, а також встановити вимоги до фінансування заходів по захисту інформації.

У ***п'ятій*** групі питань проводиться вибірка засобів захисту і визначення їх характеристик.

У цій групі необхідно відповісти перш за все на такі питання:

– Які загрози мають бути прибрані і в якій мірі?

– Які зони об'єкту мають бути захищені і якою мірою?

– За допомогою яких засобів має бути реалізований захист?

– Яка має бути повна вартість реалізації захисту і витрати на експлуатацію з урахування потенційних загроз?

– Які спільні функції зачіпаються?

– Який новий персонал потрібний?

– Яка кваліфікація потрібна для виконання цих обов'язків?

– Яка вартість доступна?

– Який виграш в безпеці буде отриманий при збільшенні бюджету?

Основні проблеми, які вирішують при цьому: проведення організаційної роботи для підвищення ефективності, працездатності реалізованих програм, систем, які реалізуються, та їх функціонування; розробка організаційних схем; розробка правил робіт.

Шоста група питань відноситься до впровадження і використання вибраних заходів захисту. При вирішенні цих питань необхідно відповісти на три основних питання:

– Який пріоритет секретних об'єктів?

– Як буде впливати реалізація програми захисту інформації на плани підприємства?

– Які додаткові ресурси будуть потрібні?

Складнощі, які виникають при вирішенні цих питань наступні: необхідність уникнення конфліктів із-за ресурсів, розробка планів реалізації і запобігання конфліктам при розвитку системи захисту.

Сьома група питань – контроль й управління системою захисту.

Управління захистом – це контроль за розподілом інформації у відкритих системах і каналах. Він здійснюється для забезпечення функціонування засобів і механізмів захисту: фіксація виконання функцій і стану механізмів захисту, фіксація подій, пов'язаних з порушенням захисту.

При цьому необхідно постійно вирішувати такі питання:

– Який має бути склад фахівців для ефективної роботи групи контролю?

– Чи є стандарти безпеки і секретності інформації?

– Чи ідентифіковані всі вразливі точки об'єкту?

– Які покращення можна провести, аби зробити систему захисту більш працездатною і ефективною?

– Яка періодичність контролю?

Проведені дослідження відповідей на поставлені питання показують, що вони не мають чіткої межі. На питання можна дати декілька однотипних відповідей, що може привести до неякісної

оцінки. Суворі правила, закладені в експертні системи, не дають оптимального рішення.

Прийнявши припущення – відповідь несе в собі деяку нечіткість, можна прийти до висновку, що для експертної системи необхідно використовувати апарат нечіткої логіки [9, 10]. Тоді відповідно до отриманих відповідей, використовуючи апарат нечіткої логіки, експертна система ухвалює оптимальне і обгрунтоване рішення.

Вихідними даними експертної системи будуть наступні рекомендації:

– СЗІ можна не застосовувати.

– Застосовувати слабкі СЗІ.

– Застосовувати сильні СЗІ.

– Застосовувати особливі СЗІ.

Ці рекомендації також є нечіткими поняттями, і кожна має свою приналежність (функцію приналежності) до нечіткої множини.

Тоді приналежність рекомендацій до нечіткої множини визначається за допомогою індексу нечіткості (рис. 1).

Як згадувалося вище, всі питання згруповані по темах. Питань в темі є декілька, на питання може бути декілька відповідей (по умові приймається лише одна відповідь). Відповіді мають свою приналежність до нечіткої безлічі відповідей. Відповіді типу «Важко відповісти» мають приналежність μ=0, 1, решта відповідей мають приналежність μ=0, 0,33, 0,66, 1.

Із відповідей на питання складається нечітка множина, в якій кількість стовпців дорівнює кількості питань, а кількість рядків дорівнює кількості тем.

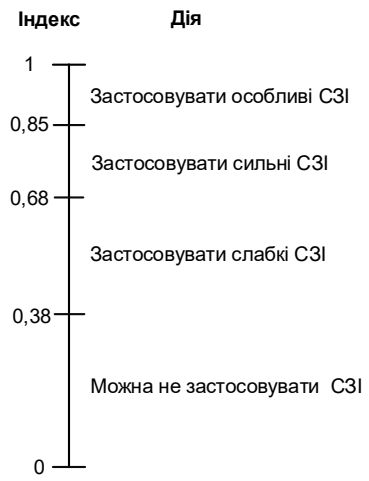

Рис. 1. Рекомендації до нечіткої множини

Використовуючи нечітку множину, визначається узагальнена відносна відстань Хеммінга [10, 11], а потім – індекс нечіткості, по якому видається експертна оцінка.

Висновки

1. Запропоновано комп'ютерну експертну методику і тести, що дозволяють точніше і об'єктивніше оцінювати економічну ефективность системи захисту інформації.

2. Визначено сім груп питань, на підставі яких експертна система ухвалює рішення про доцільність прийняття системи захисту інформації.

3. Використовуючи апарат нечіткої логіки визначається узагальнена відносна відстань Хеммінга, а потім – індекс нечіткості, по якому видається експертна оцінка.

Список літератури:

1. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Комплексні системи захисту інформації : навч. посібник. Вінниця: ВНТУ, 2017. 120 с.

2. Толюпа С.В., Самохвалов Ю.Я., Цьопа Н.В. Комплексні системи захисту інформації спеціальних об'єктів та методика їх оцінки. *Сучасний захист інформації.* 2014. № 1. С. 81–88.

3. Богуш В.М., Кудін А.М. Моніторинг систем інформаційної безпеки. Київ : ДУІКТ, 2006. 414 с.

4. Толюпа С.В., Іванова О.М., Демченко І.О. Підходи до проектування та оцінки ефективності системи захисту інформації в автоматизованих системах обробки та передачі даних. *Сучасний захист інформації.* 2013. № 1. С. 25–30.

5. Толюпа С.В., Борисов І.В. Методика оцінки комплексної системи захисту інформації на об'єкті інформаційної діяльності. *Сучасний захист інформації.* 2013. № 2. С. 43–48.

6. Сірченко Г.А. Задачі забезпечення цілісності та доступності інформаційних об'єктів в комунікаційних мережах. *Захист інформації.* 2010. № 2. С. 49–54.

7. Браіловський М.М., Лазарєв Г.П., Хорошко В.О. Захист інформації у банківській діяльності. Київ: Поліграф Консалтинг, 2004. 216 с.

8. Хорошко В.О., Кудінов В.А. Методичний підхід до формалізації задачі оцінювання ефективності системи захисту інформаційної системи ОВС України. *Захист інформації.* 2004. № 4. С.11–18.

9. Потій О.В., Лєншин А.В. Основні положення математичного апарату суб'єктивної логіки та його застосування для оцінки рівня зрілості систем забезпечення безпеки інформації. *Радіотехніка.* 2005. Тематичний випуск *Інформаційна безпека*. Харків : Харківський національний університет радіоелектроніки. С. 144–160.

10. Ус С.А. Методи прийняття рішень : навч. посібник. Донецьк : Національний гірничий університет, 2012. 212 с.

11. Волошин О.Ф., Мащенко С.О. Моделі та методи прийняття рішень : навч. посібник. 3-є вид., перероб. Київ: Видавництво Людмила, 2018. 292 с.

Rozorinov H.M., Sirchenko I.A. AN EXPERT ESTIMATION OF EFFICIENCY OF THE INFORMATION DEFENCE SYSTEMS APPLICATION IN THE NETWORKS OF AUDIOVISUAL CONTENT DISTRIBUTION

Methodology and tests are offered for the expert economic estimation of efficiency of application of the information security systems in the networks of audiovisual content distribution.

It is shown that at the economic estimation of the system except charges on the system it is necessary also to take into account cooperation between subsystems that is included in the composition (levels of defence, borders of defence and all that).

In accordance with this methodology it is necessary to answer on seven groups of questions, on the basis of that a consulting model makes decision about expedience of acceptance of the information security system. The analysis of information security system requirements is conducted in accordance with the analysis of orientation of the activity, by functions and procedures of information defence on an object.

However at the analysis of these questions there are such basic problems: access control to vulnerable and secret information; profiles of access secrecy: providing and creation of conscious attitude toward secrecy in organization, development of documentation that determines politics in relation to secrecy on the basis of normative documents. It is thus necessary to take into account specific difficulties and first of all to them it follows to take distribution of priorities for information that requires defence, by determination of relative vulnerability and secrecy of information. Except it, to the basic problems that arise up at the receipt of answers for by the set questions, it is possible to take changes in technologies of defence, that can be used by both malefactors and defenders of information, and also to set requirements to financing of events on information security.

Complications that arise up at the decision of these questions related also to the necessity of avoidance of conflicts from resources, developments of realization plans and prevention of conflicts at development of the defence system.

The analysis of answers for by the set questions shows that they do not have a clear limit. On a question it is possible to give a few of the same type answers, that can result in an off-grade estimation. The severe rules stopped up in consulting models do not give an optimal decision.

Accepting supposition, that an answer carries in itself some unclearness, drawn conclusion, that for a consulting model it is necessary to use the vehicle of fuzzy logic. Then in accordance with the got answers, using the vehicle of fuzzy logic, a consulting model accepts an optimal and reasonable decision.

Using a fuzzy set, the generalized relative distance of Hamming is determined, and then is an index of unclearness, on that an expert estimation is given out.

Key words: *information security, network, fuzzy set, estimation of efficiency.*