КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2019.3.97103
УДК 316.776:004.58

Рой Яніна Володимирівна
Кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0002-8353-1856
djanetta378@gmail.com

Мазур Наталія Петрівна
Кандидат педагогічних наук, доцент доцент кафедри інформаційної та кібернетичної безпеки Київський університет імені Бориса Грінченка, м. Київ, Україна
OrcID 0000-0001-7671-8287
n.mazur@kubg.edu.ua

Рябчун Олена Петрівна
Інженер І категорії
Державний науково-дослідний інститут спеціального зв'язку та захисту інформації України
OrcID0000-0002-4400-0112
santalen@bigmir.net

СТРАТЕГІЯ ВИЗНАЧЕННЯ ГІПОТЕТИЧНОГО НАПРЯМУ ПІДВИЩЕННЯ РІВНЯ НЕБЕЗПЕКИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Анотація. В даній статті до розгляду пропонується математичний апарат порівняльного аналізу множини загроз державних інформаційних ресурсів (ДІР), який поєднує в собі методи і підходи щодо оцінки їх якісних та кількісних показників. Головною особливістю дослідження є те, що запропонований підхід до вирішення задачі вибору не вимагає повного відновлення принципу оптимальності, а дозволяє обмежитись лише інформацією, що буде достатньою для виділення "еталонної вибірки". Сутність процедури ранжирування полягає у тому, що експерт розташовує загрози ІР в тому порядку, який на його погляд є найбільш раціональним. Кожному з них експерт приписує конкретні числа з натурального ряду - ранги. При цьому найвищий ранг отримує та загроза, яка має найбільший пріоритет. Порядкова шкала, яку буде отримано в результаті ранжирування, повинна задовольняти умові рівності кількості рангів кількості ранжируваних загроз. В даному випадку найменш небезпечній загрозі буде відповідати менше чисельне значення комплексної оцінки. При цьому метод безпосередньої оцінки використовується в тих випадках, коли існує чітка різниця між загрозами (альтернативами), що розглядаються, та (або) вони піддаються безпосередньому вимірюванню, так як мають однакову природу. Суть методу полягає у тому, що експерт повинен кожну загрозу, яка розглядається, поставити на певне місце у відповідності до ступеня наявності тієї чи іншої властивості, або у відповідності із запропонованим цим же експертом коефіцієнтом значимості. В даному випадку більше чисельне значення комплексної оцінки відповідає найменш небезпечній загрозі. Основним математичним методом оцінки небезпеки загроз із "генеральної сукупності" класів загроз ІБ обрано метод формування та дослідження узагальнених показників (критеріїв), результати комплексного поєднання яких дозволяють з'ясувати тенденції якісного зростання їх значущості. Для підвищення достовірності результатів оцінки рівнів потенціальної небезпеки кожної загрози із "генеральної сукупності" класів загроз ІБ застосовуються методи експертних оцінок. Застосування запропонованого методу сприятиме зменшенню часу на оцінку стану захищеності інформаційних ресурсів та дозволить, по-перше, визначити найбільш значимі загрози, які можуть заподіяти найбільшого збитку інформаційній безпеці й, по-друге, першочергово спрямувати на них необхідні засоби та заходи захисту.

Ключові слова: державні інформаційні ресурси, інформаційна безпека, метод аналізу ієрархій.

ISSN 2663 - 4023

1. ВСТУП

Необхідність убезпечення державами світу ІКТ та ІТС, а також захисту ними власного інформаційного ресурсу (ІР) та власної інфраструктури передусім від втручань і загроз антропогенного і техногенного характеру, що реалізуються зловмисниками останнім часом через атаки нульової доби, атаки на провайдерів та на мобільні пристрої тощо, потребує [1]:

- прийняття певних законодавчих актів, а також розробки стратегії виконання низки організаційних та інженерно-технічних заходів із забезпечення інформаційної безпеки;
- створення відповідних органів, функції, повноваження та зона відповідальності яких має визначатися з урахуванням історичних традицій, національних пріоритетів і вітчизняного законодавства;
- вирішення найбільш важливих і загальних та, в тому чи іншому формулюванні, найбільш пріоритетних задач, що передбачають посилення боротьби з міжнародним тероризмом, забезпечення безпеки інформаційного і кіберпросторів, а також захисту критично-важливих об'єктів національної інфраструктури.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Вирішення завдання визначення гіпотетичного напряму підвищення небезпеки загроз інформаційній безпеці (ІБ) полягає в тому, щоб за відомим розташуванням у $L-$ вимірному просторі показників (критеріїв) існуючих загроз обгрунтувати напрямок зміни потенціальної небезпеки загроз з "генеральної сукупності" класів загроз – $\Phi_{\max}$, тобто тенденції якісного зростання їх значущості, а також визначити рівень такої небезпеки для кожної із загроз. Це здійснюється шляхом перетворення системи координат таким чином, щоб її початок співпадав зі значенням уявної точки, що відповідає найменш небезпечній загрозі з "еталонної вибірки" – "нульовому варіанту", або інакше, відповідно до умов нашої задачі, – "найкращому еталону".

Відносно неї ведуться подальші обчислювання.

Подібні завдання раніше вирішувались виключно за допомогою кількісних методів [2,3]. При цьому, як правило:

1) виникала необхідність у порівнянні досліджуваних загроз за сукупністю характеристик і в ранжируванні їх у порядку зменшення (зростання) отриманих результатів;

2) загальний показник виражався як нечітко задана функція впливу на нього кожного з часткових показників – якісних характеристик.

В даноій статті до розгляду пропонується математичний апарат порівняльного аналізу множини загроз державних інформаційних ресурсів (ДІР), який поєднує в собі методи і підходи щодо оцінки їх якісних та кількісних показників.

У формалізованому вигляді зазначена задача зводиться до такої.

Відома деяка множина загроз $i=\overline{1,N}$, яка отримала назву "генеральної сукупності" класів загроз ІБ. Кожна з цих загроз характеризується відповідними показниками – "j", де $j=\overline{1,L}$, й має встановлений за певним правилом пріоритет. За основні вихідні дані будемо використовувати показники (критерії) існуючих загроз, що характеризують: можливість порушення конфіденційності, цілісності, доступності та спостережності інформації.

ISSN 2663 - 4023

Необхідно за сукупністю показників ранжирувати досліджувані загрози в порядку зменшення або зростання їх значимості й за певним коефіцієнтом, шляхом порівняння вибрати загрозу, яка може завдати найменшої шкоди.

Рішення зводиться до реалізації таких послідовних етапів [4-5]:

а) розробки процедури визначення пріоритетності актуальних загроз ІБ та формування з них впорядкованої "еталонної вибірки". При цьому та із загроз, яка в ряді переваг стоятиме першою і матиме серед інших найнижчий пріоритет (тобто завдає найменшої шкоди), обирається за "нульовий варіант";

б) формування технології визначення рівня небезпеки загроз із "генеральної сукупності" класів загроз ІБ, яка застосовуючи основні постулати методу "прогресуючого еталону" та основні показники існуючих загроз дозволить визначити коефіцієнти рівнів потенціальної небезпеки обраних для дослідження загроз із "генеральної сукупності". При цьому та із загроз, яка може заподіяти найбільшого збитку й на яку необхідно першочергово спрямувати засоби та заходи захисту обирається шляхом порівняння значень коефіцієнтів серед множини загроз із "генеральної сукупності" класів загроз ІБ ($i = \overline{1, N}$).

Можливі наслідки отриманих рішень визначаються з точки зору збалансування таких факторів:

підвищення рівня потенціальної ефективності існуючої системи захисту;

забезпечення максимальної економічної та виробничої доцільності проведення заходів з модернізації існуючої системи захисту інформації;

збільшення допустимого часу експлуатації існуючої СЗІ і т. інше:

В процесі вирішення загальної задачі вибору приймають участь: особа, що приймає рішення, експерти та консультанти [6]. Особою, що приймає рішення (ОПР), називають людину, яка має певну мету, що в свою чергу служить мотивом щодо постановки задачі та пошуку її вирішення. ОПР, як правило, є компетентним спеціалістом у своїй галузі та має досвід діяльності в ній, наділена необхідними повноваженнями й несе відповідальність за прийняте рішення. У задачі прийняття рішення, що вирішується в даній роботі, основна функція ОПР полягає у виділенні з "генеральної сукупності" класів загроз ІБ (N) деякої підмножини – "еталонної вибірки" актуальних загроз (Q), а з неї – одного варіанту, найбільш значимої загрози, яка може заподіяти найбільшого збитку й на яку мають бути першочергово спрямовані засоби та заходи захисту. Відсутність хоча б одного із зазначених елементів ("еталонної вибірки" актуальних загроз із "генеральної сукупності" класів загроз ІБ, а також принципу визначення їх оптимальності) – позбавляє сенсу задачу в цілому.

Експертом називають спеціаліста, який має інформацію про задачу, що розглядається, але не несе безпосередньої відповідальності за результат її вирішення. Експерт дає оцінки конкуруючим варіантам із "еталонної вибірки", розташовуючи їх при цьому в ряд переваг, що необхідні для вирішення задачі вибору. Консультантом називають спеціаліста в галузі теорії вибору та прийняття рішення. Консультант розробляє модель вихідної задачі, процедуру прийняття рішення, організує роботу особи, яка приймає рішення, та експертів під час пошуку рішення. Інакше кажучи консультант – це той спеціаліст (спеціалісти), який готує необхідну базу вихідних даних для експертів та ОПР.

Головною особливістю дослідження є те, що запропонований підхід до вирішення задачі вибору не вимагає повного відновлення принципу оптимальності, а дозволяє

ISSN 2663 - 4023

обмежитись лише інформацією, що буде достатньою для виділення "еталонної вибірки".

Математичним виразом принципу оптимальності служитиме цільова функція вибору – $\Phi(R_{заг})$. Вона характеризує кожну загрозу із "еталонної вибірки" й обчислюється при заданих варіантах множини (Q).

Для вирішення задачі обгрунтування пріоритетності актуальних загроз інформаційній безпеці та формування з них впорядкованої "еталонної вибірки" найдоцільнішим на наше бачення є застосування методів експертних оцінок [41 – 42]. Найпоширенішими серед них й до того ж такими, що шляхом перетворення формалізованої інформації в форму, яка буде зручною для прийняття певного управлінського рішення, дозволять проводити порівняльний аналіз множини відомих загроз ІБ, є як відомо методи:

а) безпосередньої оцінки;

б) аналізу ієрархій;

в) ранжирування, тощо .

При цьому метод безпосередньої оцінки використовується в тих випадках, коли існує чітка різниця між загрозами (альтернативами), що розглядаються, та (або) вони піддаються безпосередньому вимірюванню, так як мають однакову природу. Суть методу полягає у тому, що експерт повинен кожну загрозу, яка розглядається, поставити на певне місце у відповідності до ступеня наявності тієї чи іншої властивості, або у відповідності із запропонованим цим же експертом коефіцієнтом значимості. В даному випадку більше чисельне значення комплексної оцінки відповідає найменш небезпечній загрозі.

Метод аналізу ієрархій (МАІ) є систематичною процедурою для ієрархічного представлення загроз, які визначають суть будь-якої проблеми. Він поєднує в собі процедури синтезу різних міркувань, отримання пріоритетності критеріїв та знаходження альтернативних рішень. В основі цього методу лежить присвоювання загрозам числових оцінок на основі експертного опитування. На першому етапі застосування МАІ відбувається структурування проблеми у вигляді ієрархії. Далі встановлюються пріоритети критеріїв, відбувається оцінювання кожної альтернативи й виявляється найважливіша. Порівняння відбувається у відповідності з вербальною шкалою попарно, враховуючи вплив порівнюваних зразків на загальну для них характеристику. Для порівнювання зразків формуються матриці порівнянь. При їх заповнюванні слід
відповісти на такі запитання:

наскільки найменш небезпечна загроза небезпечніша від інших за одним із вибраних критеріїв (показників);

наскільки, стосовно основної мети, критерій (показник) $К_1$ важливіший критерію (показника) $К_к$, де к – кількість можливих критеріїв (показників).

В результаті порівняння загроз формується квадратна матриця, елементи якої мають властивість оберненої симетричності. З групи матриць парних порівнянь формується набір локальних пріоритетів, з яких, в свою чергу, синтезуються глобальні (загальні для всіх) пріоритети. Для визначення альтернативи під час порівняння можуть бути використані судження як одного експерта, так і колективні погляди групи експертів.

Застосування МАІ в якості методологічної основи в методиках порівняльної оцінки загроз ІР дає можливість:

ISSN 2663 - 4023

а) виключити застосування апарату регресійного аналізу;

б) більш об'єктивно враховувати якісні характеристики в корисності системи тощо.

Сутність процедури ранжирування полягає у тому, що експерт розташовує загрози ІР в тому порядку, який на його погляд є найбільш раціональним. Кожному з них експерт приписує конкретні числа з натурального ряду - ранги. При цьому найвищий ранг отримує та загроза, яка має найбільший пріоритет. Порядкова шкала, яку буде отримано в результаті ранжирування, повинна задовольняти умові рівності кількості рангів кількості ранжируваних загроз. В даному випадку найменш небезпечній загрозі буде відповідати менше чисельне значення комплексної оцінки.

Метод ранжирування застосовують у випадках, коли:

необхідно упорядкувати будь-які системи у просторі в ситуаціях, коли цікавляться не тільки порівнянням ступеня визначеності будь-якої їх властивості, а лише взаємним просторовим розташуванням цих систем;

необхідно упорядкувати системи у відповідності з якою-небудь властивістю, але при цьому непотрібно виконувати його точне вимірювання тощо.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Основним математичним методом оцінки небезпеки загроз із "генеральної сукупності" класів загроз ІБ обрано метод формування та дослідження узагальнених показників (критеріїв), результати комплексного поєднання яких дозволяють з'ясувати тенденції якісного зростання їх значущості. Для підвищення достовірності результатів оцінки рівнів потенціальної небезпеки кожної загрози із "генеральної сукупності" класів загроз ІБ застосовуються методи експертних оцінок.

Застосування запропонованого методу сприятиме зменшенню часу на оцінку стану захищеності інформаційних ресурсів та дозволить, по-перше, визначити найбільш значимі загрози, які можуть заподіяти найбільшого збитку інформаційній безпеці й, по-друге, першочергово спрямувати на них необхідні засоби та заходи захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Н.Ф. Казакова, та Т.І. Соклакова, «Удосконалення методу моніторингу рівня інформаційної безпеки у спеціальних сегментах національної інформаційної інфраструктури», Бионика интеллекта, № 1(84), с. 56-64, 2015.

[2] Г.К.Круг, Статистические методы в инженерных исследованиях. Москва, СРСР: Высшая школа, 1983.

[3] Н.Н. Бек, и Д.И. Голенко, Статистические методы оптимизации в экономических исследованиях. Москва, СРСР: Статистика, 1971.

[4] В.Л. Бурячок, «Методика обґрунтування рішення на модернізацію зразків зенітних ракетних комплексів шляхом порівняльної воєнно-економічної оцінки їх потенціальної ефективності», дис. канд. наук, ЦНДІ ОВТ ЗС України, Київ, Україна, 2001.

[5] С.А. Саркисян, Теория прогнозирования и принятия решений. Москва, СРСР: Высшая школа, 1977.

[6] В.Л. Бурячок, М.М. Мітрахович, та М.М. Луханін, «Методичні аспекти експертного аналізу зразків техніки при вирішенні задач прогнозування їх застосування та розвитку», Наука і оборона, №4, с. 38-43, 2002.

[7] В.Л. Бурячок, та Я.В. Невойт, «Метод визначення найбільш значимих загроз із «генеральної сукупності загроз» інформаційним ресурсам на підставі їх якісних та кількісних показників», Сучасний захист інформації, №3, с. 18-21, 2015.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (3), 2019
ISSN 2663 - 4023

Yanina Vl. Roy
PhD, Associate Professor of the Department of Information and cyber security Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID 0000-0002-8353-1856
djanetta378@gmail.com

Nataliia P. Mazur
PhD, Associate Professor the Department of Information and cyber security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID 0000-0001-7671-8287
n.mazur@kubg.edu.ua

Olena Pt. Riabchun
Engineer Category I
State Research Institute of the Special
communication and information protection of Ukraine, Kyiv, Ukraine
OrcID 0000-0002-4400-0112
santalen@bigmir.net

STRATEGY OF DETERMINATION OF THE HYPOTHETIC DIRECTION OF INCREASING THE RISK OF INFLAMMATION OF THE INFRASTRUCTURE SAFETY

Abstract. In this article, a mathematical apparatus for comparative analysis of the set of threats of state information resources (DIR) is proposed for consideration, which combines methods and approaches to assess their qualitative and quantitative indicators. The main feature of the study is that the proposed approach to solving the problem of choice does not require a complete restoration of the principle of optimality, but allows to limit only information that will be sufficient to select the "reference sample". The essence of the ranking procedure lies in the fact that the expert poses the threat of an IP in the order that, in his opinion, is the most rational. For each of them the expert assigns specific numbers from a natural series - ranks. In this case, the highest rank receives the threat that has the highest priority. The order scale to be obtained as a result of ranking should satisfy the condition of equality of the number of ranks of the number of ranked threats. In this case, the less complex value of the numerical value will correspond to the least dangerous threat. The essence of the method lies in the fact that the expert must put each threat considered in a certain place in accordance with the degree of availability of one or another property, or in accordance with the proposed by the same expert, the coefficient of significance. In this case, the larger value of a complex assessment corresponds to the least dangerous threat. The basic mathematical method for assessing the threat of threats from the "general population" of the IB classes of threats is the method of formation and research of generalized indicators (criteria), the results of complex combination of which determine the trends of qualitative growth of their significance. Methods of expert assessments are used to increase the reliability of the results of assessing the levels of potential hazards of each threat from the "general population" of IB threat classes. The application of the proposed method will reduce the time to assess the state of the security of information resources and will allow, firstly, to identify the most significant threats that could inflict the greatest damage to information security and, secondly, to direct them the necessary means and safeguards.

Key words: state information resources, information security, method of analysis of hierarchies.

REFERENCES

[1] N.F. Kazakova, and T.I. Soklakova, “Udoskonalennia metodu monitorynhu rivnia informatsiinoi bezpeky u spetsialnykh sehmentakh natsionalnoi informatsiinoi infrastruktury [Improvement of the method of monitoring the level of information security in special segments of the national information infrastructure]”, Bionics of Intellect, no.1(84), pp. 56-64, 2015. (In Ukrainian)

[2] G.K.Krug, Statisticheskie metody v inzhenernyh issledovanijah [Statistical Methods in Engineering Studies]. Moskow, Vysshaja shkola, 1983, 216p. (In Russian)

[3] N.N. Bek, and D.I. Golenko, Statisticheskie metody optimizacii v jekonomicheskih issledovanijah [Statistical methods of optimization in economic research]. Moskow, Statistika, 1971, 136 p. (In Russian)

[4] V.L. Buryachok, Metodyka obgruntuvannia rishennia na modernizatsiiu zrazkiv zenitnykh raketnykh kompleksiv shliakhom porivnialnoi voienno-ekonomichnoi otsinky yikh potentsialnoi efektyvnosti [A methodology for substantiating the decision to modernize samples of anti-aircraft missile systems by comparative military-economic evaluation of their potential effectiveness], Thesis for Science. Cand.Tech.Sci., ZNDI of the Army of the Armed Forces of Ukraine, Kyiv, 2001. (In Ukrainian)

[5] S.A. Sarkisjan, Teorija prognozirovanija i prinjatija reshenij [Theory of forecasting and decision-making]. Moskow, Vysshaja shkola, 1977, 112 p. (In Russian)

[6] V.L. Buryachok, M.M. Mitrachovich, and M.M. Lukhanin, “Metodychni aspekty ekspertnoho analizu zrazkiv tekhniky pry vyrishenni zadach prohnozuvannia yikh zastosuvannia ta rozvytku [Methodical aspects of expert analysis of engineering samples in solving problems of forecasting their application and development]”, Science and Defense, no.4, pp. 38-43, 2002. (In Ukrainian)

[7] V.L. Buryachok, and Y.V. Nevoyt, “Metod vyznachennia naibilsh znachymykh zahroz iz «heneralnoi sukupnosti zahroz» informatsiinym resursam na pidstavi yikh yakisnykh ta kilkisnykh pokaznykiv [Method of determining the most significant threats from the "general set of threats" to information resources on the basis of their qualitative and quantitative indicators]”, Modern Information Protection, no.3, pp.18-21, 2015. (In Ukrainian)