УДК [001.8/.816/.817] + 001.92 + [371.315.5/.315.6/.335] +655.52

Ігор Миколайович Козубцов *(канд. техн. наук, с.н.с.)*
Леся Михайлівна Козубцова
Володимир Вікторович Куцаєв
Тетяна Павлівна Терещенко
Військовий інститут телекомунікацій та інформатизації, Київ, Україна

МЕТОДИКА ОЦІНКИ КІБЕРНЕТИЧНОЇ ЗАХИЩЕНОСТІ СИСТЕМИ ЗВ'ЯЗКУ ОРГАНІЗАЦІЇ

В статті проаналізовано відкриті джерела мережі Інтернет на наявність методики оцінки кібернетичної захищеності інформаційно-телекомунікаційної системи зв'язку організації. Встановлено, що на даний час відсутня аналогічна мелодика оцінки кібернетичної захищеності інформаційно-телекомунікаційної системи зв'язку організації. В даний час для оцінки кіберзахищеності системи зв'язку застосовується система якісних показників. Для оцінки кіберзахищеності необхідно застосовувати кількісні показники, використання яких забезпечує більш об'єктивну оцінку. На цій підставі авторським колективом запропоновано мелодику оцінки кібернетичної захищеності інформаційно-телекомунікаційної системи зв'язку організації на початковому етапі. Наукова новизна одержаного результату полягає в тому, що авторами вирішено наукову задачу з розробки методики оцінки кібернетичної захищеності інформаційно-телекомунікаційної системи зв'язку організації. Її наукова новизна підтверджується відсутністю у відкритому доступі аналогічних, подібних методик, а отже пріоритет наукової новизни визначається за авторами даної статті.

Ключові слова: *методика, оцінка, кібернетична захищеність, система зв'язку, організація.*

Втуп

Постановка проблеми і зв'язок її з важливими науковими завданнями. Питання оцінки кібернетичної захищеності інформаційно-телекомунікаційної системи зв'язку будь-якої організації є актуальним, проте і досі воно не вирішене.

В даний час для оцінки кіберзахищеності інформаційно-телекомунікаційної системи зв'язку застосовується система якісних показників. Для кількісної оцінки кіберзахищеності необхідно застосовувати кількісні показники, використання яких забезпечує більш об'єктивну оцінку.

Рішення цього завдання передбачає розробку підходу для визначення кількісного показника рівня кіберзахищеності і трансформація в кількісні значення якісного показника заданого рівня захищеності та проведення оцінки отриманих результатів. Для отримання кількісної оцінки показника кіберзахищеності можуть бути використані апарат теорії ймовірності, теорії масового обслуговування і теорії надійності, що дозволяють з достатньою точністю описувати (моделювати) процеси, що протікають в захищеній інформаційній системі.

Тому, авторський колектив поставив за мету розробити мелодику оцінки кібернетичної захищеності інформаційно-телекомунікаційної системи зв'язку організації на початковому етапі. Складність рішення наукової задачі полягає в тому, що до складу методики можуть входити набагато більше складових, а наявні міждисциплінарні зв'язки ускладнюють їх вираховування на практиці. Внаслідок цього розрахункова частина стає надто громіздкою, збір всіх вихідних даних затребує істотного часу. Проте інколи достатньо 5-7 параметрів, які достатньо перевірити на виконання вимог та з певною ймовірністю встановити початковий рівень кібернетичної захищеності дослідної системи.

Аналіз останніх досліджень і публікацій. Аналіз відкритих джерел в мережі Інтернет по ключовим словам методика оцінки кібернетичної захищеності системи зв'язку організації не дав позитивного результату, що свідчить про недослідженість даного питання на відміну від питання захищеності системи зв'язку. І це не випадково, а цілком логічно, оскільки проблема забезпечення кібернетичної захищеності системи зв'язку організації постала на початку нового тисячоліття з розвитком стратегій дій та операцій в кібернетичному просторі [1]. Поряд з цим спостерігається зацікавленість у дослідників оцінки захищеності системи зв'язку.

Авторами роботи [2] запропоновано здійснювати оцінку рівня захищеності комп'ютерних мереж шляхом побудови графа атак.

А у статті [3] - можливий варіант механізму оцінювання ступеня захищеності спеціальних ІТС з точки зору дій системного адміністратора та дій, що виконуються системою аналізу ступеня захищеності системи. Встановлено проблемні питання оцінювання загроз безпеці інформації в спеціальних інформаційно-телекомунікаційних систем за метою реалізації з позицій забезпечення її конфіденційності, цілісності і доступності. Зазначимо, що в роботах [2, 3] запропоновані рішення не забезпечують саме оцінити рівень кібернетичної захищеності інформаційно-телекомунікаційної системи зв'язку організації.

Мета статті. В розробці методики оцінки кібернетичної захищеності інформаційно-

телекомунікаційної системи зв'язку організації методом експертного анкетування відповідальних кіберфахівців організації.

Результат дослідження

Методика оцінки рівня кіберзахищеності організації призначена для того, щоб керівники і фахівці кібернетичної безпеки організації могли оцінити рівень кіберзахищеності інформаційно-телекомунікаційної системи зв'язку організації та без додаткових матеріальних і тимчасових витрат виконати вимоги чинного законодавства України із забезпечення кіберзахисту організації.

Методика побудована на процесі інтерв'ювання різних фахівців (керівників, системних адміністраторів, інших фахівців кібернетичної безпеки), що складається з опитувального листа, який, у свою чергу, розбитий на групи, які дозволяють оцінити рівень кіберзахищеності інформаційно-телекомунікаційної системи зв'язку організації з виконання вимог: організації кібернетичного захисту; з технічного захисту (витоки по технічних каналах; загрози несанкціонованого доступу); з програмного захисту; рівень захищеності (модель порушника; типи загрози; базові моделі загроз).

Значення рівня захищеності (вірогідність) для кожного критерію обчислюється за формулою:

$$Z = \frac{(Y1 + Y2)}{20}, \qquad (1)$$

де Y1 – оцінка вірогідності початкової захищеності системи зв'язку організації, яка приймає значення: Y1 = 10 високий рівень захищеності; Y1 = 0 низький рівень захищеності; Y2 – оцінка вірогідність виникнення загрози, приймає значення: Y2 = 10 реалізація загрози низька; Y2 = 5 реалізація загрози середня; Y2 = 0 реалізація загрози висока.

ЕТАП 1 «Оцінка виконання вимоги з організації кібернетичного захисту системи зв'язку організації»

Група «1. Вимоги з організації кібернетичного захисту системи зв'язку організації», в якому основний акцент зроблений на виконання вимог по організаційному захисту (KZ1).

ЕТАП 2 «Оцінка кібернетичної захищеності системи зв'язку організації від загрози витоку інформації щодо керування правами доступу (адміністрування)»

ЕТАП 2.1 «Оцінка кібернетичної захищеності системи зв'язку організації від загрози витоку акустичній інформації керування правами доступу».

Група «2.1. Оцінка захищеності системи зв'язку організації від загрози витоку акустичній інформації акустичній інформації керування правами доступу». Дана група призначена для визначення рівня захищеності кібернетичної системи від витоків по акустичному каналу інформації про права до доступу (KZ2.1).

ЕТАП 2.2 «Оцінка захищеності системи зв'язку організації від загрози витоку візуальній інформації про права доступу».

Група «2.2. Оцінка захищеності системи зв'язку організації від загрози витоку візуальній інформації що носить інформацію про права доступу». Дана група призначена для визначення рівня захищеності інформаційної системи від просочувань візуальної інформації що носить інформацію про права доступу (KZ2.2).

ЕТАП 2.3 «Оцінка кіберзахищеності системи зв'язку організації від загрози знищення, розкрадання апаратних засобів, матеріальних носіїв інформації шляхом фізичного несанкціонованого доступу».

Група «2.3. Оцінка кіберзахищеності системи зв'язку організації від погроз знищення, розкрадання апаратних засобів, носіїв інформації шляхом фізичного доступу до елементів». Дана група призначена для визначення рівня захищеності інформаційної системи від погроз знищення, розкрадання апаратних засобів (KZ2.3).

ЕТАП 2.4 «Оцінка спроможності забезпечення кіберзахищеності системи зв'язку організації шляхом розмежування прав доступу».

Група «2.4. Оцінка кіберзахищеності по виконанню технічних вимог» (KZ2.4).

ЕТАП 3 «Оцінка кіберзахищеності системи зв'язку організації від загроз несанкціонованого доступу»

ЕТАП 3.1 «Оцінка кіберзахищеності системи зв'язку організації від заходів розвідки кібернетичної інфраструктури». Група «3.1. Оцінка кіберзахищеності системи зв'язку організації від заходів розвідки кібернетичної інфраструктури» (KZ3.1). Мета етапу. Здійснити розрахункову оцінку можливої реалізації розвідки комунікацій противником шляхом мережевого сканування.

ЕТАП 3.2 «Оцінка кіберзахищеності системи зв'язку організації від заходів кібернетичного впливу на функціонування кібернетичної інфраструктури». Група «3.2. Оцінка кіберзахищеності системи зв'язку організації від заходів кібернетичного впливу на функціонування кібернетичної інфраструктури» (KZ3.2). Мета етапу полягає здійснити розрахункову оцінку можливої захищеності системи зв'язку ЗСУ від впливу дій DOS та DDOS атаки, яку можна на початку атаки виявити анти сканерами та нейтралізувати спеціальними заходами та обладнанням.

ЕТАП 3.3 «Оцінка спроможності забезпечення кіберзахищеності системи зв'язку організації шляхом застосування системи кібернетичного захисту інфраструктуру»

Група «3.3. Оцінка спроможності забезпечення кіберзахищеності системи зв'язку організації шляхом застосування системи кібернетичного захисту інфраструктуру». У табл. 1 представлений опитувальний лист (KZ3.3).

Мета. Здійснити розрахункову оцінку можливої захищеності системи зв'язку ЗСУ від впливу дій шкідливого СПЗ, яке можливо виявити антивірусними програмами за умови відсутності настання інциденту нульового дня.

ЕТАП 3.4 «Оцінка кіберзахищеності системи зв'язку організації з виконанню вимог з програмного захисту». Група «3.4. Оцінка рівня захищеності системи зв'язку організації з виконанню програмних вимог» (KZ3.4).

ЕТАП 4 «Моделі внутрішнього і

зовнішнього порушника». Група «4. Розробка моделей порушника». Моделлю порушника є опис типів зловмисників, які своїми діями або без дією, навмисно або випадково здатні завдати збитку інформаційній системі [4]. В роботі [5] надано опис мотиваційного портрету учасника кібернетичного протистояння, як захисника так і порушника кіберпростору. Зазвичай складають наступну модель порушника:

внутрішні (кінцеві користувачі системи, персонал обслуговуючий технічні засоби, програмне забезпечення, керівники, співробітники служби безпеки, допоміжний персонал);

зовнішні (технічний персонал по обслуговуванню обчислювальної техніки, відвідувачі, представники інших організацій, фахівці, обслуговуючі спеціалізоване програмне забезпечення).

ЕТАП 5 «Загальна оцінка рівня кіберзахищеності ІТС системи зв'язку організації»

Визначаємо порядок визначення вагових коефіцієнтів. Для цього необхідно здійснити попарне порівняння критеріїв експертної оцінки. Результат попарного порівняння критеріїв експертної оцінки подано, як приклад на рис. 1.

	1	2	3	4	5	6	7	8	9	10	Si	Ki - ваговий
1	1	0	0	0	0	0	0	0	0	1	2	**0,02**
2	2	1	1	0	0	0	0	0	0	0	4	**0,04**
3	2	1	1	0	0	0	0	0	0	0	4	**0,04**
4	2	2	2	1	0	0	0	0	0	0	7	**0,07**
5	2	2	2	2	1	0	0	0	0	0	9	**0,09**
6	2	2	2	2	2	1	0	0	0	0	11	**0,11**
7	2	2	2	2	2	2	1	1	2	2	18	**0,18**
8	2	2	2	2	2	2	1	1	2	2	18	**0,18**
9	2	2	2	2	2	1	1	0	1	2	15	**0,15**
10	1	2	2	2	2	1	1	0	0	1	12	**0,12**
∑												**1**

Рис. 1. Попарне порівняння критеріїв експертної оцінки

Оцінка загального рівня кіберзахищеності системи зв'язку організації. Слід зазначити, що дотримання всіх вимог, перерахованих вище, є необхідною умовою для безпечного функціонування системи зв'язку. Оцінка загального рівня кіберзахищеності системи зв'язку організації (∑KZ) обчислюється за формулою (2) розрахунку середньозваженого значення.

$$\sum KZ=\frac{(K_1\cdot KZ_1)+(K_2\cdot KZ_{2.1})+(K_3\cdot KZ_{2.2})+(K_4\cdot KZ_{2.3})+(K_5\cdot KZ_{2.4})+(K_6\cdot KZ_{3.1})+(K_7\cdot KZ_{3.2})+(K_8\cdot KZ_{3.3})+(K_9\cdot KZ_{3.4})+(K_{10}\cdot KZ_4)}{KZ_1+KZ_{2.1}+KZ_{2.2}+KZ_{2.3}+KZ_{2.4}+KZ_{3.1}+KZ_{3.2}+KZ_{3.3}+KZ_{3.4}+KZ_4} \quad (2)$$

Розраховуючи середньозважене значення забезпечується реалізувати адаптивний підхід, оскільки кожна група показників KZ має різний характер і вагу впливу на загальний показник (∑KZ).

Висновки та перспективи подальших досліджень

Таким чином, можна сформулювати наступні висновки:

на даний час відсутня загальна методика оцінки кібернетичної захищеності інформаційно-телекомунікаційної системи зв'язку організації. Поясненням цьому може бути в тому, що до складу методики можуть входити набагато більше складових по мірі збільшення загроз, а наявні міждисциплінарні зв'язки ускладнюють їх вираховування на практиці;

методика ґрунтується на процесі інтерв'ювання різних фахівців (керівників, системних адміністраторів, інших фахівців кібернетичної безпеки), що складається з опитувального листа;

визначені питання у опитувальному листі не є догмою, та можуть бути відкоректовані (уточнені) за потреби.

Наукова новизна одержаного результату. Авторами вирішено наукову задачу з розробки ефективної методики оцінки кібернетичної захищеності системи зв'язку організації.

Методика ґрунтується на процесі інтерв'ювання різних фахівців (керівників, системних адміністраторів, інших фахівців кібернетичної безпеки), що складається з опитувального листа, який, у свою чергу, розбитий на групи, що дозволяють оцінити рівень кіберзахищеності інформаційно-телекомунікаційної системи зв'язку організації: вимоги з організаційного захисту; вимоги з технічного захисту (витоки по технічних каналах; загрози несанкціонованого доступу); вимоги з програмного захисту; рівень захищеності (модель порушника; типи загрози; базові моделі загроз).

Наукова новизна підтверджується відсутністю у відкритому доступі аналогічних, подібних методик, а отже пріоритет наукової новизни визначається за авторами даної статті.

Література

1. Козубцов І.М. Стратегія гри в кібернетичному просторі / І.М. Козубцов, Л.М. Козубцова // Матеріали Міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» (Київ, 17– 20 листопада 2015 р.). – Київ. Державний університет телекомунікацій, 2015. – Том III Розвиток інформаційних технологій – С. 52 – 54.

2. Степашкин М.В. Оценка уровня защищенности компьютерных сетей на основе построения графа атак / И.В. Котенко, М.В. Степашкин // Труды международной научной школы "Моделирование и анализ безопасности и

риска в сложных системах". – Спб., 2006. – С. 150 – 154. **3. Бурячок В.Л.** Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем // Науково-технічний журнал «Захист інформації». – 2011. – №3(52). – С. 19 – 27. **4. Анин Б.Ю.** Защита компьютерной информации / Б.Ю. Анин. – СПб.: БХВ-Петербург, 2000. – 376 с. – ISBN 5-8206-0104-1. **5. Козубцов І.М.** Про мотиваційний портрет учасники кібернетичного протистояння / І.М. Козубцов // Актуальні проблеми розвитку науки і техніки: Матеріали першої міжнародної науково-технічної конференції. Збірник тез. – К.: ДУТ, 2015. – С.208 – 211.

МЕТОДИКА ОЦЕНКИ КИБЕРНЕТИЧЕСКОЙ ЗАЩИЩЕННОСТИ СИСТЕМЫ СВЯЗИ ОРГАНИЗАЦИИ

***Игорь Николаевич Козубцов** (канд. техн. наук, с.н.с.)*
Леся Михайловна Козубцова
Владимир Викторович Куцаева
Татьяна Павловна Терещенко

Военный институт телекоммуникаций и информатизации, Киев, Украина

В статье проанализированы открытые источники сети Интернет на наличие методики оценки кибернетической защищенности информационно-телекоммуникационной системы связи организации. Установлено, что в настоящее время отсутствует аналогичная мелодика оценки кибернетической защищенности информационно-телекоммуникационной системы связи организации. В настоящее время для оценки кіберзахищеності системы связи применяется система качественных показателей. Для оценки кіберзахищеності необходимо применять количественные показатели, использование которых обеспечивает более объективную оценку. На этом основании авторским коллективом предложено мелодику оценки кибернетической защищенности информационно-телекоммуникационной системы связи организации на начальном этапе. Научная новизна полученного результата заключается в том, что авторами решено научную задачу разработки методики оценки кибернетической защищенности информационно-телекоммуникационной системы связи организации. Ее научная новизна подтверждается отсутствием в открытом доступе аналогичных, подобных методик, а следовательно приоритет научной новизны определяется авторами данной статьи.

***Ключевые слова:** методика, оценка, кибернетическая защищенность, система связи, организация.*

METHOD OF ASSESSMENT OF THE CIBERNETIC PROTECTION OF THE ORGANIZATION COMMUNICATION SYSTEM

***Igor M. Kozubtsov** (Candidate of Technical Sciences, Senior Research Fellow)*
Lesja M. Kozubtsova
Volodymyr V. Kutsayev
Tetyana P.Tereshchenko
Military institute of telecommunications and informatization of the, Kiev, Ukraine

The article analyzes the open sources of the Internet for the presence of methods of assessment of cybernetic security of information and telecommunication system of the organization. It is established that at present there is no similar melody of assessment of cybernetic security of information and telecommunication system of the organization. Currently, to assess kardahians communication system, a system of quality indicators. To assess kardahians it is necessary to apply the quantitative indicators, the use of which provides a more objective assessment. On this basis, the authors ' team proposed a melodica assessment of cybernetic security of information and telecommunication system of the organization at the initial stage. The scientific novelty of the obtained result lies in the fact that the authors solved the scientific task of developing a methodology for assessing the cybernetic security of the information and telecommunication system of the organization. Its scientific novelty is confirmed by the absence of similar methods in open access, and therefore the priority of scientific novelty is determined by the authors of this article.

***Keywords:**methodology, assessment, cyber security, communication systems, organization*

References

1. Kozubtsov I.M., Kozubtsova L.M. (2015) Strategy game in cyberspace [Stratehiia hry v kibernetychnomu prostori] // Materials of International scientific-technical conference "Modern information and telecommunication technologies" (Kyiv, 17– 20 November 2015). – Kiev. State University of telecommunications . – Volume III Development of information technology – p. 52 – 54. **2. Stepashkin M.V., Kotenko I.V.** (2006) Assessment of the level of security of computer networks based on the graph of attacks [Otsenka urovnya zaschischennosti kompyuternyih setey na osnove postroeniya grafa atak] // Proceedings of the international school of science "Modeling and analysis of safety and risk in complex systems". – SPb. P. 150 – 154. **3. Buriachok V.L.** (2011) The algorithm for estimating the security of special information-telecommunication systems [Alhorytm otsiniuvannia stupenia zakhyshchenosti spetsialnykh informatsiino-telekomunikatsiinykh system] // Scientific-technical magazine "information security". No. 3(52). P. 19 – 27. **4. Anin B.Yu.** (2000) Protection of computer information [Zaschita kompyuternoy informatsii]. SPb.: Bkhv-Petersburg. 376 p. ISBN 5-8206-0104-1. **5. Kozubtsov I.M.** (2015) About motivational portrait of the participants of the cyber opposition [Pro motyvatsiinyi portret uchasnyky kibernetychnoho protystoiannia] // Actual problems of development of science and technology: proceedings of the first international scientific-technical conference. The book of abstracts. K. FLS. P. 208 – 211.