УДК 621.391

Юрій Іванович Вілюха
Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна

КІЛЬКІСНЕ ОЦІНЮВАННЯ РІВНЯ НЕБЕЗПЕКИ КІБЕРНЕТИЧНИХ ЗАГРОЗ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

У статті розглядається приклад кількісного оцінювання рівня небезпеки кібернетичних загроз інформаційно-телекомунікаційної системи (далі - ІТС) на прикладі ІТС оперативного угруповання військ з урахуванням рівня критичності складових ІТС як об'єкта захисту від кібернетичних загроз. Автором статті при розробці методичного підходу до оцінювання рівня небезпеки кібернетичних загроз враховується не тільки саму загрозу і імовірність її появлення але й критичність складових ІТС щодо впливу кібернетичних загроз і можливий збій у функціонуванні ІТС та збиток в обміні інформації.

Ключові слова: *інформаційно-телекомунікаційна система, кібернетична загроза, критичність складових ІТС.*

Вступ

За висновками фахівців кіберзагроз і засобів їх реалізацій (кібератак) продовжується тенденція того, що кіберпростір використовують для ескалації конфліктів між державами; провідні країни світу з метою підвищення рівня кібербезпеки створюють нові структурні підрозділи, проводять їх злагодження та вдосконалюють навички, нарощують свої можливості у сфері ведення кіберборотьби, при цьому головна увага акцентується на активному пошуку уразливостей систем управління важливих держаних та військових об'єктів [1].

З метою нейтралізації (мінімізації) впливу кібернетичних загроз на інформаційно-телекомунікаційну систему (далі – ІТС) у ЗС України продовжують створюватися підрозділи кібернетичного захисту в ІТС. Разом з тим, вибір складу сил і засобів цих підрозділів на рівні оперативного командування слабо обгрунтований, не відповідає рівню небезпеки кібернетичних загроз ІТС ОУВ, а методичні підходи, за допомогою яких проводиться їх оцінювання не враховують специфіки військової ІТС.

Так, існуючі методичні підходи до оцінювання рівня кібернетичних загроз на ІТС, ґрунтуються на оцінюванні збитку від їх реалізації у абсолютних одиницях: вартості втрачених коштів, часу, рейтингу підприємства, об'ємі втраченого прибутку, інформації тощо. Такий підхід неприпустимий під час оцінювання збитку на військові ІТС, тому що у такому разі збитком будуть людські життя, втрачені важливі об'єкти внаслідок порушення або втрати управління військами (силами), зброєю (бойовими засобами).

Найбільш прийнятним методичним підходом до оцінювання рівня кібернетичних загроз на військову ІТС автор статті вважає [2]. У зазначеному підході, на відміну від інших здійснюється визначення не абсолютного, а відносного збитку від реалізації кіберзагроз, що цілком допустимо для військових ІТС. Крім того, автором підходу враховується такий показник, як ступінь критичності складових власне ІТС. З погляду системи управління, кожна складова ІТС може характеризуватися рівнем критичності, який відображає ступінь неможливості реалізації основних функцій ІТС щодо забезпечення обміну інформацією або вимог кібернетичної безпеки ІТС у разі порушення (припинення) її функціонування.

Постановка проблеми. Відомо, що для визначення адекватного складу сил та засобів підрозділів кіберзахисту необхідно оцінити рівень небезпеки кібернетичних загроз ІТС ОУВ. Тому основна ціль даного дослідження – запропонувати методичний підхід кількісної оцінки рівня небезпеки кібернетичних загроз ІТС ОУВ

Аналіз остатніх досліджень і публікацій. Сьогодні оцінюванню рівня кібернетичної небезпеки систем різного цільового призначення приділяється все більше уваги у багатьох галузях науки і техніки [3–6]. Детально огляд методів оцінювання рівня небезпеки наведено в праці [6], де зазначено, що найбільшого поширення набули метод на основі байєсівських мереж, методологія "Risk Management Guide for Information Technology Systems", метод "VAR" (Value at Risk), методика "TRA" (Threat and Risk Assessment), методика "FRAP" (Facilitated Risk Analysis Process), стандарт ISO/IEC 27005:2008 (Information technology – Security techniques – Information security risk management) та ін.

Виклад основного матеріалу дослідження. На сьогоднішній день відсутнє єдине розуміння такого поняття, як "небезпека кібернетичної загрози", що зумовлює значні труднощі під час розроблення методичного підходу до її оцінювання. Тому, в контексті цього дослідження, під рівнем небезпеки кібернетичної загрози ІТС

ОУВ будемо розуміти міру небезпеки для інформаційно-телекомунікаційної системи.

Автори [6] оцінюють рівень небезпеки за виразом (1):

$$Z = P \cdot У \cdot (1 - P_{бар}), \quad (1)$$

де: Z - рівень небезпеки загроз для ІТС; P – імовірність реалізації загрози; У – збиток від загрози; $P_{бар}$ – ступінь спротиву захисного бар'єру, яка характеризує імовірність його подолання.

У цьому дослідженні не розглядається питання використання захисного бар'єру від загроз, тому у подальшому рівень небезпеки буде розглядатися як міра небезпеки для ІТС, що характеризується ймовірністю появи такої загрози та величиною нормованого відносного збитку від кібернетичної загрози на ІТС ОУВ.

Можемо визначити цільову функцію, яка має вигляд:

$$Z_{ITC} = f\left(P, Q\right), \quad (2)$$

де: Z_{ITC} – рівень небезпеки кібернетичних загроз для ІТС ОУВ; P – імовірність реалізації кібернетичної загрози; Q – нормований відносний збиток від кібернетичної загрози на ІТС ОУВ.

За умов незалежності загроз та адитивності їх наслідків, рівень небезпеки від кібернетичних загроз ІТС ОУВ визначається як [7, 8]:

$$Z_{ITC} = P_i \times Q_i + \ldots + P_n \times Q_n = Z_i + \ldots + Z_n = \sum_{i=1}^{n} Z_i \quad (3)$$

де: $Z_i = P_i * Q_i$ – рівень небезпеки i-ї кібернетичної загрози; P_i – імовірність реалізації i-ї кібернетичної загрози; Q_i – відносний нормований збиток від i-ї кібернетичної загрози на ІТС; n – кількість кібернетичних загроз.

Імовірність реалізації i-ї кібернетичної загрози P_i визначається як:

$$P_i = \frac{N_i}{N_{\Sigma i}}, \quad (4)$$

де N_i – кількість випадків реалізації i-ої кібернетичної загрози; $N_{\Sigma i}$ – загальна кількість усіх випадків виникнення i-ої кібернетичної загрози.

Тоді вираз (3) матиме вигляд:

$$Z_{ITC} = \frac{N_i}{N_\Sigma} Q_i + \ldots + \frac{N_n}{N_\Sigma} Q_n = \frac{1}{N_\Sigma} \sum_{i=1}^{n} N_i \cdot Q_i. \quad (5)$$

Вочевидь, що рівень відносного збитку від різних кібернетичної загроз на різні складові ІТС буде мати різні значення. Тому, надалі визначаються складові ІТС, що можуть стати об'єктом подібних загроз та оцінюється рівень небезпеки від i–ї кібернетичної загрози на кожну складову ІТС. Типовий склад ІТС ОУВ визначається як $O=\{O_j\}$ (припустимо, що він буде кінцевим та лічильним, $j = \overline{1,m}$).

Ураховуючи адитивний характер відносного збитку i-ої кібернетичної загрози на ІТС ОУВ, його можна представити як [2]:

$$Q_i = \frac{q_{ij}}{\sum_{i=1}^{n} q_{im}} + \ldots + \frac{q_{nm}}{\sum_{i=1}^{n} q_{nm}} = q_{ij}^* + \ldots + q_{nm}^* = \sum_{j=1}^{m} q_{ij}^*, \quad (6)$$

де q_{ij} – відносний збиток i-ої кібернетичної загрози на j-у складову частину ІТС ОУВ; q_{ij}^* – нормований відносний збиток i-ої кібернетичної загрози на j-у складову частину ІТС ОУВ; n – кількість кібернетичних загроз; m – кількість складових ІТС ОУВ.

Для зручності формалізації сформуємо матрицю рівня відносного збитку актуальних кібернетичних загроз $I=\{I_i\}$, які здійснюють вплив на множину складових ІТС $O=\{O_j\}$ (таблиця 1).

Таблиця 1 – Матриця рівня відносного збитку актуальних кібернетичних загроз $I^*=\{I_i\}$, які здійснюють вплив на складові ІТС $O=\{O_j\}$.

		$O=\{O_j\}, j=1,m$			
		O_1	O_2	…	O_m
$I^*=\{I_i\}, i=1,n$	I_1	q_{11}	q_{12}	…	q_{1m}
	…	…	…	…	…
	I_i	q_{i1}	q_{i2}	…	q_{im}
	…	…	…	…	…
	I_n	q_{n1}	q_{n2}	…	q_{nm}

Пропонується застосувати метод експертних оцінок. Оцінювання цим методом – наочне, просте та зручне. З цією метою кожний експерт оцінює рівень критичності j-ї складової ІТС ОК за 8- бальною системою (при цьому 1 – найнижчий рівень критичності, 8 – найвищий). Далі знаходиться сума балів експертів для кожної складової ІТМ, ранжирується рівень критичності складових ІТС ОУВ відповідно до суми балів, причому найвищий ранг, 1, отримує той, хто набрав більшу суму балів.

Можливість використання результатів ранжирування ступеня критичності складових ІТС ОУВ для подальших розрахунків проводиться на підставі розрахунку коефіцієнта конкордації експертних оцінок за відомою формулою:

$$W = \frac{12S}{k^2 \cdot (m^3 - m)}, \quad 0 \le W \le 1, \quad (7)$$

де W– коефіцієнт конкордації, S – сума квадратів відхилення оцінок рангів кожної складової ІТС від середнього значення; k – кількість експертів; m – кількість складових ІТС ОК.

При цьому вважається, що якщо $W=0$, то результати експертів повністю неузгоджені, якщо $W=1$, то результати експертів повністю узгоджені.

Нормування оцінки рівня критичності складових ІТС ОК здійснюється за виразом:

$$a_j = \frac{\overline{a}_j}{\sum_{j=1}^{m} \overline{a}_j}, \quad (8)$$

де: a_j – нормована оцінка рівня критичності *j*-ї складової ІТС ОК; $\overline{a}_i$ – середнє значення рівня критичності *j*-ї складової ІТС за оцінкою експертів.

З урахуванням зазначеного вище, рівень відносного збитку від *i*-ої кібернетичної загрози на ІТС ОУВ (6) матиме вигляд:

$$Q_i = q_{ij} \cdot a_j + \ldots + q_{nm} a_m = \sum_{j=1}^{m} q_{ij} a_{ij}, \quad (9)$$

де: q_{ij} – нормоване значення рівня відносного збитку *i*-ої кібернетичної загрози на *j*-у складову частину ІТС ОК; *n* – кількість кібернетичних загроз; *m* – кількість складових ІТС ОК; a_j – нормоване значення рівня критичності *j*-ї складової частини ІТС ОК.

Якщо підставити вираз (9) у вираз (5), то рівень небезпеки від *i*-х кібернетичних загроз ІТС ОК можна визначити як:

$$Z_{ITC} = \frac{N_i}{N_\Sigma} Q_i + \ldots + \frac{N_n}{N_\Sigma} Q_n = \frac{N_i \sum_{j=1}^{m} q_{ij} a_{ij}}{N_\Sigma} + \ldots + \frac{N_n \sum_{j=1}^{m} q_{nm} a_{nm}}{N_\Sigma} = \frac{1}{N_\Sigma} \sum_{i=1}^{n} N_i \sum_{j=1}^{m} q_{ij} a_{ij} \quad (10)$$

Отже, за виразом (10) можна здійснити оцінювання рівня небезпеки кібернетичних загроз для ІТС ОУВ з урахуванням таких факторів, як імовірність появи таких загроз (P_i), нормованого відносного збитку (Q_i), а також рівня критичності складових частин ІТС ОК (a_j). При цьому, зазначений методичний підхід можливо застосовувати для будь-якої кількості кібернетичних загроз та для ІТС будь-якого складу.

Надалі, з урахуванням визначеної множини найбільш розповсюджених кібернетичних загроз $I=\{I_i\}$ та типового складу ІТС ОК $O=\{O_j\}$, для наочності розрахунків рівня відносного збитку від *i*-ї кібернетичної загрози на ІТС ОК, перетворимо вираз (10) у матричний вигляд:

$$Q_i = q_{ij} \cdot a_j + \ldots + q_{nm} a_m = \sum_{j=1}^{m} q_{ij} a_{ij} \Rightarrow \left.\begin{array}{l} Q_1 = q_{11} \cdot a_1 + \ldots + q_{nm} a_m \\ Q_2 = q_{21} \cdot a_1 + \ldots + q_{nm} a_m \\ \ldots \\ Q_m = q_{i1} \cdot a_1 + \ldots + q_{nm} a_m \end{array}\right\} \Rightarrow \begin{vmatrix} Q_1 \\ Q_2 \\ \ldots \\ Q_n \end{vmatrix} =$$
$$= \begin{vmatrix} q_{11} & q_{12} & \ldots & q_{nm} \\ q_{21} & q_{22} & \ldots & q_{nm} \\ \ldots & \ldots & \ldots & \ldots \\ q_{n1} & q_{n2} & \ldots & q_{nm} \end{vmatrix} \times \begin{vmatrix} a_1 & a_2 & \ldots & a_m \end{vmatrix} \Rightarrow \left|Q\right| = \left|q\right| \times \left|a\right|, \quad (11)$$

де: $\left|Q\right|$ - матриця-стовпець нормованих значень відносного збитку *i*-ї кібернетичної загрози на ІТС ОУВ розмірністю *n*x*1*; $\left|q\right|$ – матриця нормованих значень відносного збитку *i-ї* кібернетичної загрози на *j-y* складову частину ІТС ОУВ розмірністю *nxm*; $\left|a\right|$ - матриця-рядок нормованих значень рівня критичності *j*-ї складової частини ІТС ОК розмірністю *1*x*m*.

З урахуванням (11), перетворимо вираз (5) у матричний вигляд:

$$Z_i = P_i \cdot Q_i = \frac{N_i}{N_\Sigma} Q_i \Rightarrow \left.\begin{array}{l} Z_1 = \frac{N_1}{N_\Sigma} Q_1 = \frac{N_1}{N_\Sigma}\left(q_{11} \cdot a_1 + \ldots + q_{1m} a_m\right) \\ Z_2 = \frac{N_2}{N_\Sigma} Q_2 = \frac{N_2}{N_\Sigma}\left(q_{21} \cdot a_1 + \ldots + q_{2m} a_m\right) \\ \ldots \\ Z_i = \frac{N_i}{N_\Sigma} Q_i = \frac{N_i}{N_\Sigma}\left(q_{ij} \cdot a_j + \ldots + q_{im} a_m\right) \\ \ldots \\ Z_n = \frac{N_n}{N_\Sigma} Q_n = \frac{N_n}{N_\Sigma}\left(q_{nm} \cdot a_m + \ldots + q_{nm} a_m\right) \end{array}\right\} \Rightarrow$$
$$\Rightarrow \begin{vmatrix} Z_1 \\ Z_2 \\ \ldots \\ Z_n \end{vmatrix} = \begin{vmatrix} P_1 & 0 & \ldots & 0 \\ 0 & P_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & P_n \end{vmatrix} \times \begin{vmatrix} Q_1 \\ Q_2 \\ \ldots \\ Q_n \end{vmatrix} = \left|P\right| \times \left|q\right| \times \left|a\right| = \frac{1}{N_\Sigma} \times \left|N\right| \times \left|q\right| \times \left|a\right|, \quad (12)$$

де: $\left|Z\right|$ – матриця-стовпець рівня небезпеки від *i*-ї кібернетичної загрози на ІТС ОУВ розмірністю *n*x*1*; $\left|P\right|$ – матриця ймовірностей реалізації *i*-ї кібернетичної загрози розмірності *n*x*n*; $\left|N\right|$ – матриця кількості випадків виникнення і-ї кібернетичної загрози розмірності *n*x*n*; $\left|q\right|$ – матриця нормованих значень відносного збитку *i*-ї кібернетичної загрози на *j*-у складову частину ІТС розмірністю *n*x*m*; $\left|a\right|$ – матриця-рядок нормованих значень рівня критичності j-ї складової частини ІТС розмірністю *1*x*m*.

Висновки й перспективи подальших досліджень

Таким чином, комплексна природа кібернетичних загроз вимагає розглядати їх як загрози процесам управління, що відбуваються у ІТС, а не лише інформації, яка циркулює в таких системах.

Автором запропонований удосконалений методичний підхід до оцінювання рівня небезпеки кібернетичних загроз ІТС шляхом урахування оцінки рівня критичності складових ІТС. Це дозволило визначити пріоритети для складових ІТС як об'єктів захисту від кібернетичних атак різних видів, що в подальшому може стати вихідними даними для визначення раціонального складу сил та засобів кібернетичного захисту ІТС ОУВ.

Література

1. Олійник В.М., Самойленко Ю.В., Кузьмук Р.Р. Про кіберентичну безпеку України: проект Закону України. Київ, 2013. 16 с. **2. Буйко К.В.,** Пантюхова Ю.В. Подходы к оценке уровня промышленной безопасности в организациях, эксплуатирующих опасные производственные объекты. Безопасность труда в промышленности, 2010. № 10. С. 42–46. **3. Гаршин А.Ю.,** Иванченко О.В., Мащенко Е.Н. Методика оценки уровня опасности морской критической инфраструктуры Системи озброєння і військова техніка, 2010. № 3 (23). С.107 –109. **4. Нечунаев В.М.** Оценка рисков информационной

безопасности корпоративной информацинной системы: доклады ТУСУР. Томск, 2009. №1 (19). Ч.2. С. 51–53. **5. Корченко А.Г.,** Иванченко Е.В. Казмирчук С.В. Анализ и определения понятия риска для его интерпретации в области информационной безопасности. Науково-технічний журнал "Захист інформації", 2010. №3. С. 1–5. **6. Аверченков В.І.,** М.Ю. Рытов М.Ю., Гайнулин Т.Р. Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса-Хоффмана. Вестник Брянского государственного технического университета, 2008. №1 (17). С. 61–66. **7. Домарев В.В.** Безопасность информационных технологий. Методология создания систем защиты: монография. К. ТОВ "ТНД", 2002. 688 с. **8. Сташевський, З.П.,** Грицюк Ю.І. обгрунтування показника якості функціонування комплексної системи захисту інформації. Вісник Національного технічного університету України, 2014. №56. С. 137–143. **9. Корт С.С.** Теоретические основы защиты информации: учебное пособие. М. Гелиос АРВ, 2004. 240 с. **10. Горницька Д.А.,** Волянська В.В., Корченко А.О. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки. Науково-технічний журнал "Захист інформації", 2012. №1. С. 108–121.

КОЛИЧЕСТВЕННАЯ ОЦЕНКА УРОВНЯ ОПАСНОСТИ КИБЕРНЕТИЧЕСКИХ УГРОЗ ИНФОРМАЦИОННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ

Юрий Иванович Вилюха

Центральный –научно-исследовательский институт Вооруженных Сил Украины , Киев, Украина

В статье рассматривается пример количественного оценивания уровня опасности кибернетических угроз информационно-телекоммуникационной системе (далее - ИТС) на примере ИТС оперативной группировки войск с учетом уровня критичности составляющих ИТС как объекта защиты от кибернетических угроз. Автором статьи при разработке методического подхода к оценке уровня опасности кибернетических угроз учитывается не только саму угрозу и вероятность ее появление, но и критичность составляющих ИТС, возможный сбой в функционировании ИТС и ущерб в обмене информации.

Ключевые слова: *информационно-телекоммуникационная система, кибернетическая угроза, критичность составляющих ИТС.*

.

QUANTITATIVE EVALUATION OF THE RISK OF DANGERS OF CIBERNETIC DAMAGES OF THE INFORMATION AND TELECOMMUNICATION SYSTEM

Yuri Ivanovich Vylyuha

Central Scientific-Research Institute of the Armed Forces of Ukraine, Kiev, Ukraine

The article considers an example of a quantitative estimation of the level of danger of cybernetic threats to the information and telecommunication system (ITS) on the example of the ITS of the operational grouping of troops, taking into account the level of criticality of components of ITS as an object of protection against cybernetic threats. The author of the article when developing a methodical approach to assessing the level of danger of cybernetic threats takes into account not only the threat itself and the probability of its occurrence, but also the criticality of the components of the ITS, the possible failure of the functioning of ITS and the damage to the exchange of information.

Keywords: *information and telecommunication system, cybernetic threat, criticality of ITS components*

References

1. Mykus S.A. Models of production-logical derivation of knowledge in the automation of decision support process in the system of communication control / S.A. Mykus // Proceedings of the University, NUOU - 2017. - No. 5 (144). - p. C.47-53. **2. Mykus S.A**. QS-system for controlling the properties of a multiservice network / S.A. Mikus, Yu.V. Kravchenko, RK Murasov // Mathematics. Information Technology. Education: a collection of materials of the IV International Scientific and Practical Conference (Lutsk - Svityaz, June 5-7, 2017). - 2017. - P. 52-55. **3. Mykus S.A.** The Concept of Functionally Sustainable Management of Information Resources in the Telecommunication System of Military Purposes / S.A. Mykus, OA Mashkov, Yu.V. Kravchenko // Proceedings of the scientific and technical conference of young scientists "Actual problems of information technologies -2017", Kiev, 8-10 November) - 2017. - P. 37- 38. **4. Savchenko V.A.** Model of multilevel decision support system real time based on intellectual integration / VA Savchenko // Registration, storage and data processing - 2011. - №1 (13). - p.106-112**. 5. Bronshtein I.N.** Mathematical Reference for Engineers and Students / I.N. Bronstein, K.A. Semendyayev - M.: Science, 1986. - 544 p. **1. Oliynyk VM,** Samoilenko Yu.V., Kuzmuk R.R. On Cybernetic Security of Ukraine: Draft Law of Ukraine. Kyiv, 2013. 16 p. 2. Buiko K.V., Pantyukhova Yu.V. Approaches to assessing the level of industrial safety in organizations operating hazardous production facilities. Labor safety in industry, 2010. № 10. P. 42-46. **3. Garzin A.Yu.**, Ivanchenko OV, Mashchenko E.N. Methodology for assessing the level of marine critical infrastructure hazard Arms and military equipment, 2010. No. 3 (23). P.107-109. **4. Nechunayev V.M**. Assessment of information security

risks of the corporate information system: TUSUR reports. Tomsk, 2009. №1 (19). Part 2 S. 51-53. **5. Korchenko AG,** Ivanchenko E.V. Kazmirchuk S.V. Analysis and definition of the concept of risk for its interpretation in the field of information security. Scientific and Technical Journal "Protection of Information", 2010. №3.
Pp. 1-5. **6. Averchenko V.I.,** M.Yu. Rytov M.Yu., Gainulin T.R. Optimization of the choice of composition of means of engineering technical protection of information on the basis of Clements-Hoffman model. Bulletin of the Bryansk State Technical University, 2008. Number 1 (17). Pp. 61-66. **7. Domarev V.V.** Information technology security. Methodology for creating security systems: monograph. K. "TND" LLC, 2002. 688 p. **8. Stashevsky, ZP**, Gritsyuk Yu.I. substantiation of the quality index of functioning of the complex system of information security. Bulletin of the National Technical University of Ukraine, 2014. №56. Pp. 137-143.**9. Корт С.С.** Theoretical foundations of information protection: a manual. M. Gelios ARV, 2004. 240 p. **10. Hornitskaya D.A.,** Volyanska V.V., Korchenko A.O. Determination of importance factors for expert assessment in the field of information security. Scientific and Technical Journal "Protection of Information", 2012. №1. Pp. 108-121.