DOI:**10.33099/2311-7249/2020-38-2-57-62**

УДК 621.396

Дмитро Георгійович Шевченко (кандидат військових наук)

Національний університет оборони України імені Івана Черняховського, Київ, Україна

СУКУПНІСТЬ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ЗБРОЙНИХ СИЛ УКРАЇНИ

В статті розглянуте актуальне питання удосконалення сукупності показників системи кібербезпеки в інформаційно-телекомунікаційних мережах. Проаналізовані останні дослідження і публікації з цього питання. Проведений аналіз та досвід проведення антитерористичної операції та операції Об'єднаних сил на сході України, свідчить про те, що в умовах сучасних бойових дій ефективне функціонування системи кібербезпеки в інформаційно-телекомунікаційних мережах буде у суворих часових рамках на збільшених просторових відстанях між інформаційно-телекомунікаційними вузлами та в умовах радіоелектронного й вогневого впливу противника. Також виявлено, що в загальному випадку кількість показників ефективності функціонування системи кібербезпеки в інформаційно-телекомунікаційних мережах перевищує кілька десятків. В статті проведено систематизацію та групування їх по відповідним ознакам.

В статті розглядається методичний підхід для вирішення прикладної задачі, який оснований на застосуванні методу згортки показників ефективності. Пропонується інтегральний показник ефективності та критерій оцінювання ефективності функціонування системи кібербезпеки в інформаційно-телекомунікаційних мережах Збройних Сил України.

Запропонована удосконалена сукупність показників ефективності функціонування системи кібербезпеки в інформаційно-телекомунікаційних мережах Збройних Сил України, яка на відміну від існуючих враховує додаткові показники, які обумовлені особливостями проведення операцій в сучасних умовах, а також комплексно характеризує ефективність функціонування системи кібербезпеки в інформаційно-телекомунікаційних мережах Збройних Сил України. Це дає можливість всебічно оцінити ефективність функціонування системи кібербезпеки в інформаційно-телекомунікаційних мережах Збройних Сил України в цілому, окремих елементів та її складових та їх внесок у загальний рівень ефективності функціонування системи зв'язку.

Ключові слова: *зв'язок; інформаційно-телекомунікаційна мережа; кібербезпека.*

Вступ

Постановка проблеми. Матеріальною основою системи кібербезпеки (далі – СКБ) в інформаційно-телекомунікаційних мережах (далі – ІТМ) Збройних Сил України (далі – ЗС України) є комплекси, системи та засоби автоматизації (далі – КСЗ), які об'єднують та групують з метою вирішення визначених завдань [1]. Основним стимулом її розвитку є постійне збільшення кількості викликів та загроз у кіберпросторі та відповідно розширення множини задач D, які необхідно вирішити. Це в свою чергу передбачає відповідний розвиток комплексів, систем та засобів автоматизації, програмного та інформаційного забезпечення системи кібербезпеки в ІТМ. При цьому мають місце такі взаємопов'язані процеси: процес виключення з множини D задач, які втратили актуальність; процес включення в множину D нових і модифікованих задач; процес вирішення задач множини D за їх надходженням.

Передбачається, що з оперативно-технічних міркувань визначений мінімально допустимий рівень функціональної ефективності P_d системи кібербезпеки загалом. Отже, завдання управління функціональною ефективністю системи кібербезпеки зводиться до підтримання цієї ефективності на рівні не нижче заданого

$$P_f(t) \geq P_d,\ 0 \leq t \leq \infty \qquad (1)$$

Стан системи кібербезпеки в ІТМ, при якому виконується наведена нерівність (1) – стан функціональної придатності системи. Протилежний стан визначатиме стан функціональної непридатності.

Природно, що вирішення завдання управління ефективністю має місце протягом всього

життєвого циклу системи кібербезпеки в ІТМ. Це означає, що в кожному органі управління в якому розгорнуті КСЗ, повинен бути фахівець(ці), персонально відповідальний за її вирішення, а сукупність таких фахівців в рамках СКБ в ІТМ ЗС України утворить службу управління функціональною ефективністю. Отже, існує нагальна потреба створити інструмент для оцінювання та підтримання ефективності функціонування СКБ в ІТС ЗС України.

Аналіз останніх досліджень і публікацій. Питанню дослідження ефективності функціонування СКБ в ІТС присвячено багато робіт та публікацій [2-4, 6-10].

Результати проведеного аналізу та досвід проведення АТО та ООС показали, що в умовах сучасних бойових дій ефективне функціонування системи кібербезпеки в інформаційно-телекомунікаційних мережах буде у суворих часових рамках на збільшених просторових відстанях між інформаційно-телекомунікаційними вузлами та в умовах радіоелектронного й вогневого впливу противника.

Мета статті: удосконалення сукупності показників ефективності функціонування СКБ в ІТМ ЗС України.

Виклад основного матеріалу дослідження.

Особливостями проведення операцій в сучасних умовах та факторами, які значно впливають на СКБ в ІТС ЗС України, крім відомих, у цих умовах будуть:

випереджаюча відносно пунктів управління готовність зв'язку;

вибір раціональних позицій розгортання елементів СКБ в ІТМ ЗС України, і відповідно необхідність забезпечення кібернетичної безпеки ІТМ ЗС України на великому театрі воєнних дій;

необхідність у короткий проміжок часу спланувати та змінити топологію мережі смузі операції;

складна радіоелектронна обстановка, широке застосування противником засобів РЕБ;

дотримання скритності зв'язку для максимального ускладнення ведення радіо- і радіотехнічної розвідки та РЕБ противника.

Вищезазначене зумовило необхідність удосконалення сукупності показників ефективності функціонування СКБ в ІТС ЗС України.

Ефективність функціонування СКБ в ІТС ЗС України розглядається як функціонал

$$P_f(t) = f\{R, A, O, Q, S, M, C, E, \Psi_{ду}\} \qquad (2)$$

де $\{R\}$ – множина показників розмаху;

$\{A\}$ – ступінь автоматизації;

$\{O\}$ – множина показників оперативності;

$\{Q\}$ – множина показників якості управління;

$\{S\}$ – множина показників безпеки управління;

$\{M\}$ – множина показників мобільності;

$\{C\}$ – множина показників безперервності управління;

$\{E\}$ – множина показників економічності;

$\{\Psi_{ду}\}$ – множина додаткових умов, які важко формалізуються, але які потрібно враховувати під час ведення операцій в сучасних умовах.

Для їх систематизації всі вони зведені до схеми, яка наведена на рис. 1.

Розглянемо їх детальніше.

Показники розмаху – число ланок, число об'єктів (центрів кіберзахисту), площа, яку охоплює система. Ці показники суттєві при проектуванні та оцінці СКБ в ІТС ЗС України. У цьому випадку ця група показників задана і фіксована.

Ступінь автоматизації – число автоматизованих процесів і задач, приводить до скорочення трудовитрат, скорочення штатів органів управління та військових частин.

Перелічені характеристики на жаль мало інформативні і слабо пов'язані з кінцевою метою – підвищення ефективності функціонування СКБ в ІТМ ЗС України.

Оперативність – одне з найважливіших питань властивостей систем управління військового призначення. Пропонується оцінювати її часом розв'язання завдань і функцій, ймовірністю своєчасного виконання, виграшем в оперативності. Такі показники отримали широке розповсюдження на практиці завдяки своїй простоті та наочності.

Але більш детальне вивчення вказує на присутні йому недоліки. Перший з цих показників – час розв'язання задачі. Він, очевидно, є випадковою величиною і тому характеризувати властивості системи не може. Можна говорити про математичне очікування часу розв'язання задачі. Але в цьому випадку виникають труднощі, оскільки система розв'язує множину задач і, таким чином, даний показник є вектором великої розмірності.

Виграш в оперативності може оцінюватись для однієї задачі відношенням математичних очікувань часу її розв'язання після і до автоматизації. Але для множини таких завдань побудова аналогічної оцінки ускладнюється (вона приймає векторний характер), тому наочність втрачається. Більш того, фактично цей показник оцінює не ефективність СКБ, а ефективність автоматизації.

Рис. 1. Сукупність часткових показників ефективності функціонування системи кібербезпеки в інформаційно-телекомунікаційній мережі

Заслуговує уваги показник ймовірності своєчасного розв'язання задачі. Але тут виникають труднощі, оскільки в системі вирішується не одна, а множина D задач. Крім того, говорити про час розв'язання задачі без формулювання вимог до якості її розв'язання не зовсім коректно. Більш коректно оцінювати оперативність СКБ в ІТМ в умовах, коли множина D задач, що розв'язуються, а також вимоги до часу і якості їх розв'язання задані. У цьому випадку показник оперативності визначається через показник P_f ефективності функціонування системи як

$$P_{om} = \frac{P_f}{P_{f0}}, \qquad (3)$$

де P_{f0} – показник ефективності функціонування системи, визначений за умов, що всі отримані задачі вирішені за час, не більше заданого.

Якість управління – головна властивість системи управління, що підлягає найбільш ретельній оцінці. Пропонується оцінювати її через достовірність і точність розв'язання задач, а також через ступінь використання оптимальних рішень.

У даному випадку нас цікавить якість управління в площині, яка може характеризуватись як:

бойова ефективність СКБ в ІТМ ЗС України взагалі, як оцінка P_y пристосованості системи до вирішення заданої множини D_y завдань бойового управління по мірі їх отримання за час і з якістю не гірше заданих;

функціональна ефективність інформаційно-розрахункової системи, як оцінка P_f ступеня пристосованості цієї системи до вирішення заданої множини завдань D по мірі їх отримання за час і з якістю не гірше заданих.

під час використання такого підходу достовірність та точність є частковими характеристиками окремих задач, а не системи взагалі. Ступінь використання оптимальних рішень визначається на етапі формування множин D_y та D. Треба підкреслити, що на етапі експлуатації системи вони незмінні.

Безпека управління – найважливіша властивість, що визначає умови і обмеження, в яких вирішуються задачі множин D_y та D. Вона оцінюється через:

розвідзахищеність – оцінюється як математичне очікування часу розкриття противником пункту управління;

закриття інформації – оцінюється ймовірністю розкриття інформації за час, поки та має цінність;

імітостійкість – здатність протистояти дезінформаційним діям противника;

захист від несанкціонованого доступу – здатність протистояти використанням без права доступу.

Крім перерахованих, для характеристики СКБ в ІТС ЗС України використовуються й інші показники оперативно-тактичного і економічного змісту.

Мобільність – час, що потрібний для переміщення і розгортання (згортання) у просторі [5].

Безперервність, як властивість дієздатності оцінюється гнучкістю, а саме здатністю перебудови відповідно до умов, що змінилися, тобто часом перебудови.

Стійкість – ймовірність не порушення безперервності, оцінюється через живучість (функціонування в умовах радіоелектронного та вогневого впливу), надійність і завадостійкість.

Економічність – витрати і економічний ефект.

Введений показник P_f функціональної ефективності СКБ в ІТМ ЗС України є її узагальнюючою характеристикою, яка описує найбільш загальні властивості системи і пов'язує з її ефективністю функціонування. Разом з тим, у практичній роботі використовується множина часткових показників ефективності, кожний з яких характеризує окрему властивість системи. Зазначимо, що перехід до часткових показників не тільки вимушений, але і необхідний, оскільки саме їх використання дає можливість визначити шляхи підвищення ефективності функціонування СКБ в ІТС ЗС України.

Висновки й перспективи подальших досліджень

У статті визначена удосконалена сукупність показників системи кібербезпеки в інформаційно-телекомунікаційних мережах, які обумовлені особливостями проведення операцій в сучасних умовах, а також комплексно характеризує ефективність функціонування СКБ в ІТС ЗС України. Це дає можливість всебічно оцінити ефективність функціонування СКБ в ІТС ЗС України в цілому, окремих елементів та її складових та їх внесок у загальний рівень ефективності функціонування системи зв'язку.

В перспективі планується удосконалити методику оцінювання ефективності функціонування системи кібербезпеки в інформаційно-телекомунікаційних мережах з урахуванням удосконаленої сукупності показників системи кібербезпеки в інформаційно-телекомунікаційних мережах.

Література

1. Шевченко Д.Г., А.О. Зінченко, І.Ю. Розум Комплекси, системи і засоби військових телекомунікаційних мереж. *Київ, НУОУ*. – 2019.– 320 с. **2.** Основи кібернетичної безпеки: монографія/за заг. ред. Ю. Г. Даника. Житомир. 2016. 636 с. **3.** Кіберпростір як новий вимір геополітичного суперництва: монографія/Дубов Д. В. Київ, 2015. 328 с. **4.** Світова гібридна війна: український фронт: монографія/під заг. ред. В. П. Горбуліна. Київ. 2017. 496 с. **5.** Зв'язок військовий. Терміни та визначення. ДСТУ В-3265-95. Київ: Держстандарт України. 1996. 23 с. **6.** NIST SP 800-53 National Institute of Standards and Technology. Special Publication Security and Privacy Controls for Federal information Systems and Organizations. **7.** NIST SP 800-115 National Institute of Standards and Technology. Technical issues of IS level assessment. Assessment tools, self-assessment, internal audit, external audit, evaluation, analysis of results, use of results during the development of IS organization. **8.** NIST SP 800-137 National Institute of Standards and Technology. IS monitoring in federal information systems. **9.** NIST SP 800-184 National Institute of Standards and Technology. Functions and categories of identifiers. **10.** DoD 8530.01. Department of Defense. Indicators. Defend the nation from attack. Secure national security and military systems.

СОВОКУПНОСТЬ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННЫХ СЕТЯХ ВООРУЖЕННЫХ СИЛ УКРАИНЫ

***Шевченко Дмитрий Георгиевич** (кандидат военных наук)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье рассмотрен актуальный вопрос усовершенствования совокупности показателей системы кибербезопасности в информационно-телекоммуникационных сетях. Проанализированы последние исследования и публикации по этому вопросу. Поведенный анализ и опыт проведения антитеррористической операции и операции Объединенных сил на востоке Украины, показывает, что в условиях современных боевых действиях эффективное функционирование системы кибербезопасности будет в суровых временных рамках и увеличенных пространственных расстояниях между информационно-телекоммуникационными узлами и в условиях радиоэлектронного и огневого воздействия противника. Также обнаружено, что в общем случае количество показателей эффективности функционирования системы кибербезопасности в информационно-телекоммуникационных сетях превышает нескольких десятков. В статье проведена их систематизация та группирование по соответствующим признакам.

В статье рассматривается методический подход для решения прикладной задачи, который основан на применении метода свертки показателей эффективности. Предлагается интегральный показатель эффективности критерий оценивания эффективности функционирования системы кибербезопасности в информационно-телекоммуникационных сетях Вооруженных Сил Украины.

Предложенная усовершенствованная совокупность показателей эффективности функционирования системы кибербезопасности в информационно-телекоммуникационных сетях Вооруженных Сил Украины, которая в отличие от имеющихся учитывает дополнительные показатели, которые обусловлены особенностями проведения операций в современных условиях и также комплексно характеризует эффективность функционирования системы кибербезопасности в информационно-телекоммуникационных сетях Вооруженных Сил Украины. Это дает возможность всесторонне оценить эффективность функционирования системы кибербезопасности в информационно-телекоммуникационных сетях Вооруженных Сил Украины в целом, отдельных элементов и ее составляющих и их вклад в общий уровень эффективности функционирования системы связи.

***Ключевые слова:** связь; информационно-телекоммуникационная сеть; кибербезопасность.*

THE SET OF INDICATORS OF THE CYBER SECURITY SYSTEM IN INFORMATION AND TELECOMMUNICATION NETWORKS OF THE ARMED FORCES OF UKRAINE

***Dmytro Shevchenko** (Candidate of Military Sciences)*

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The article discusses the topical issue of improving the set of indicators of the cyber security system in information and telecommunication networks. Analyzed the latest research and publications on this issue. The analysis and experience of the anti-terrorist operation and the operation of the Joint Forces in the East of

Ukraine shows that in the conditions of modern hostilities, the effective functioning of the cyber security system will be in a harsh time frame and increased spatial distances between information and telecommunication nodes and in conditions of electronic and fire exposure of the enemy.

It was also found that, in the general case, the number of indicators of the effectiveness of the functioning of the cyber security system in information and telecommunication networks exceeds several dozen. The article presents their systematization and grouping according to the relevant criteria. The article discusses a methodological approach to solving an applied problem, which is based on the application of the method of convolution of performance indicators. An integral indicator of efficiency is proposed, a criterion for assessing the efficiency of the functioning of the cyber security system in the information and telecommunication networks of the Armed Forces of Ukraine.

The proposed improved set of indicators of the effectiveness of the functioning of the cyber security system in the information and telecommunication networks of the Armed Forces of Ukraine, which, in contrast to the existing ones, takes into account additional indicators that are due to the peculiarities of conducting operations in modern conditions and also comprehensively characterizes the effectiveness of the functioning of the cyber security system in the information and telecommunication networks of the Armed Forces of Ukraine. This makes it possible to comprehensively assess the effectiveness of the functioning of the cyber security system in the information and telecommunication networks of the Armed Forces of Ukraine as a whole, individual elements and its components and their contribution to the overall level of efficiency of the communication system.

Keywords: *connection; information and telecommunication network; cyber security.*

References

1. Shevchenko D.Gh., A.O. Zinchenko, I.Ju. Rozum Kompleksy, systemy i zasoby vijsjkovykh telekomunikacijnykh merezh. Kyjiv, NUOU. 2019.– 320 s. **2.** Osnovy kibernetychnoji bezpeky: monoghrafija/za zagh. red. Ju. Gh. Danyka. Zhytomyr. 2016. 636 s**. 3.** Kiberprostir jak novyj vymir gheopolitychnogho supernyctva: monoghrafija/Dubov D. V. Kyjiv, 2015. 328 s. **4.** Svitova ghibrydna vijna: ukrajinsjkyj front: monoghrafija/pid zagh. red. V. P. Ghorbulina. Kyjiv. 2017. 496 s. **5.** Zv'jazok vijsjkovyj. Terminy ta vyznachennja. DSTU V-3265-95. Kyjiv: Derzhstandart Ukrajiny. 1996. 23 s. **6.** NIST SP 800-53 National Institute of Standards and Technology. Special Publication Security and Privacy Controls for Federal information Systems and Organizations. **7.** NIST SP 800-115 National Institute of Standards and Technology. Technical issues of IS level assessment. Assessment tools, self-assessment, internal audit, external audit, evaluation, analysis of results, use of results during the development of IS organization. **8.** NIST SP 800-137 National Institute of Standards and Technology. IS monitoring in federal information systems.**9.** NIST SP 800-184 National Institute of Standards and Technology. Functions and categories of identifiers. **10.** DoD 8530.01. Department of Defense. Indicators. Defend the nation from attack. Secure national security and military systems.