DOI:**10.33099/2311-7249/2022-43-1-25-32**

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

Леся Михайлівна Козубцова *(кандидат технічних наук)*[1]
Володимир Миколайович Подоляк *(кандидат технічних наук, доцент)*[2]
Ігор Миколайович Козубцов *(доктор педагогічних наук, старший науковий співробітник)*[1]

[1]***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[2]***Луцький національний технічний університет, Луцьк, Україна***

МЕТОДИКА РОЗРАХУНКУ ПОТРЕБ РЕСУРСНОГО ЗАБЕЗПЕЧЕННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

В науковій статті вперше запропоновано методику розрахунку потреб ресурсного забезпечення об'єктів критичної інформаційної інфраструктури. Під "потребою у забезпеченні виконання заходів кібербезпеки об'єктів критичної інформаційної інфраструктури" в статті запропоновано наступне формулювання: як необхідну кількість засобів кіберзахисту та обслуговуючого персоналу для забезпечення належного функціонування цієї системи. Потреба в розробці цієї методики виникла в результаті аналізу останніх досліджень та публікацій, що засвідчив відсутність у відкритому доступі аналогічної методики. Зазначена методика необхідна власнику об'єкта критичної інформаційної інфраструктури для своєчасного планування ресурсного забезпечення об'єктів критичної інформаційної інфраструктури. Ці дані також необхідні для забезпечення ефективного функціонування об'єкта критичної інформаційної інфраструктури, а отже виконувати свою цільову функцію. Методика включає такі ключові етапи розрахунку, а саме: потреби організації у засобів кіберзахисту; потреби у засобах кіберзахисту на випадок колапсу; остаточної потреби у засобах кіберзахисту на доукомплектування організації та відновлення на випадок колапсу; потреби у фінансовому резерві необхідного для закупівлі однотипних засобів в процесі доукомплектування та відновлення (остаточна) засобів кіберзахисту; потреби у штаті системних адміністраторів та обслуговуючого персоналу для обслуговування засобів кіберзахисту; штатної чисельності (та на випадок колапсу) системних адміністраторів та обслуговуючого персоналу необхідного для обслуговування груп засобів кіберзахисту; коефіцієнта укомплектованості засобів кіберзахисту. Дана стаття є результатом продовженням дослідження в напрямку з попереднього опису "Майбутнє безпекове середовище 2030". Результат розширює наукові межі щодо реалізації невідкладних заходів державної політики з нейтралізації загроз кібербезпеки об'єктів критичної інформаційної інфраструктури. Наукова новизна. Вперше розроблено методику розрахунку потреб ресурсного забезпечення об'єктів критичної інформаційної інфраструктури. Методика забезпечує можливість відповідальній особі у структурно-відокремлених підрозділах об'єктів критичної інформаційної інфраструктури за єдиним шаблоном розраховувати потреби ресурсного забезпечення.

Ключові слова:*. методика, розрахунок, потреби, ресурс, забезпечення, кібербезпека, об'єкт критичної інформаційної інфраструктури.*

Вступ

Постановка проблеми. Кібербезпека об'єктів критичної інформаційної інфраструктури (ОКІІ) не є сталою величиною у часі. Це є деяка функція, що залежить від множини випадкових параметрів, а саме наявності системи кібербезпеки, укомплектованості навченим (фаховим) обслуговуючим персоналом та частотою появи нових кіберзагроз. У кіберпросторі постійно відбувається протистояння «Системи захисту та кібербезпеки ОКІІ зацікавленої сторони» з «Агентами загроз» [1]. І як наслідок існує проблема забезпечення кібербезпеки ОКІІ зацікавленою стороною. Зважаючи на необхідність у вирішенні цієї пріоритетної проблеми, Концепцією розвитку сектору безпеки і оборони України визначено оперативну ціль «1.5. Удосконалення системи кібербезпеки та захисту інформації» [2, с. 33].

Першим кроком з реалізації оперативної цілі показаної в документі [2] є розробка уніфікованої методики обчислення потреб в забезпеченні виконання заходів кібербезпеки ОКІІ.

Поштовхом до необхідності обґрунтування зазначеної методики формування загального порядку розрахунку потреби у ресурсному забезпеченні виконання заходів кібербезпеки в ОКІІ став прогноз можливих негативних наслідків в наслідок колапсу в інформаційно-

телекомунікаційних системах [3; 4].

Аналіз останніх досліджень і публікацій. Дана робота націлена на реалізацію невідкладних заходів державної політики з нейтралізації загроз кібербезпеки організацій [5] та запобіганню можливих негативних прогнозів означених в попередньому описі "Майбутнє безпекове середовище 2030" [4] в результаті «гібридної війни» [6].

При обґрунтуванні потреб ресурсного забезпечення об'єктів критичної інформаційної інфраструктури для нашого дослідження цікавим є результат роботи [7, с. 321], а саме реалізація принципу розумної достатності функціонування комплексної системи захисту інформації (КСЗІ) на підприємстві. Типова залежність величини збитку підприємства (*З*) від вартості побудови КСЗІ (*В*) наведена на рис. 1.

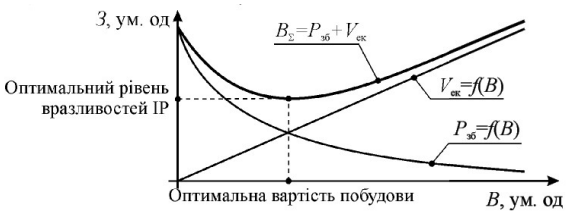

Рисунок 1. Залежність збитку підприємства від вартості побудови КСЗІ

Доказано, що із зростанням вартості побудови КСЗІ на підприємстві буде спостерігатися значне зменшення ймовірності нанесеного збитку підприємства $P_{зб}$ (зменшення вразливості інформаційного ресурсу (ІР)). З рисунку наочно видно, що застосування навіть недорогих заходів і засобів для забезпечення інформаційної безпеки підприємства (Vек) різко знижує сумарний збиток підприємства (B_Σ). Тому інвестиції в побудову КСЗІ дуже ефективні навіть в порівняно невеликих розмірах, а крива збитку (B_Σ) в деякій точці має найменше значення, яке можна вважати оптимальним.

Зростання інвестицій в побудову КСЗІ вище за оптимальне значення веде до збільшення сумарних витрат підприємства. В цьому випадку підвищення надійності роботи КСЗІ і відповідне зниження ймовірності появи збитку підприємства нівелюються надмірно високою вартістю забезпечення інформаційної безпеки підприємства.

Для обґрунтування технічної надійності ($P_{ТН}$) засобів кіберзахисту скористаємося аналогією в роботі [8] щодо оновлення і осучаснення до граничних термінів напрацювання на відмову внаслідок морального чи фізичного старіння сучасних засобів. Не можна обмежуватися тільки фізичним зносом або старінням деяких об'єктів. Для всіх без винятку об'єктів характерне моральне старіння або економічне старіння. Під фактором морального старіння розуміється настання події, коли замовнику, користувачеві або тим, хто експлуатує засоби кібербезпеки доступні об'єкти з кращими характеристиками за показником "ціна/якість" чи з кращими функціональними можливостями, ніж ті, які містяться в даній системі. Фактор економічного старіння має місце тоді, коли економічно недоцільна подальша експлуатація будь – якого об'єкта або групи об'єктів, або в цілому, хоча їх фізичний знос ще не настав і навіть не скоро настане. Для засобів кібербезпеки типова більш висока швидкість морального старіння в порівнянні з економічним, і тим більше фізичним старінням або зносом (рис. 2) [8, с. 22]. На рисунку наведені залежності від часу показників ціна/якість (*Ц/Я*) щодо морального старіння (крива $C_{МОР}(t)$), старіння через економічну недоцільність подальшої експлуатації об'єкта (крива $C_{ЕКОН}(t)$), фізичного старіння або зносу (крива $C_{ФІЗ}(t)$). Ці залежності носять якісний характер. Проте практика показує, що вже через 5 років експлуатації, внаслідок морального старіння, доцільно замінювати ряд засобів кібербезпеки на новіші, хоча фізичне старіння або знос таких об'єктів далекі від граничного стану. Це пов'язано з тим, що крива морального старіння об'єкта перетинає і перевищує гранично допустимий рівень показника Ц/Я і, отже, подальша його експлуатація нерентабельна.

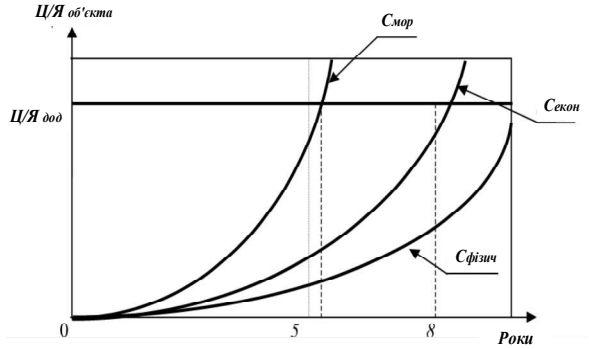

Рисунок 2. Графіки зміни швидкості морального, економічної недоцільності або фізичного старіння засобів кібербезпеки за критерієм ціна/якість (Ц/Я)

На рис. 3 подано графік кривої зміни інтенсивності відмов засобів протягом терміну експлуатації. Як практика показує І-ша фаза від 0 до t_1 має короткий проміжок часу, тому можна нею знехтувати, а за період від t_1 до t_2 (фаза ІІ) перевищує моральне старіння.

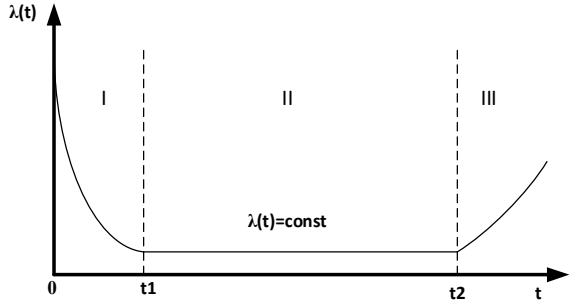

Рисунок 3. Графік кривої зміни інтенсивності відмов засобів протягом терміну експлуатації

Отже з аналізу наукових досліджень і публікацій, можна встановити, що на даний час подібна методика розрахунку потреб ресурсного

забезпечення ОКІІ відсутня. Тому існує об'єктивна необхідність у обґрунтуванні методики розрахунку потреб ресурсного забезпечення ОКІІ з урахуванням можливості настання колапсу [4].

Мета статті. Обґрунтування структури та змісту методики розрахунку потреб ресурсного забезпечення ОКІІ.

Виклад основного матеріалу дослідження

Розглянемо один з підходів до побудови методики розрахунку потреб ресурсного забезпечення ОКІІ.

В даній методиці під «потребою у забезпеченні виконання заходів кібербезпеки ОКІІ» будемо розуміти необхідну кількість засобів кіберзахисту та обслуговуючого персоналу для забезпечення належного функціонування цієї системи. Під «засобами кіберзахисту» будемо розуміти програмний, апаратно-програмний та апаратний засіб, призначений для кіберзахисту ОКІІ.

Вихідними даними для розрахунку є стан забезпеченості справними (придатними до використання за призначенням) засобами кіберзахисту відповідно до потреби в штатному режимі та на випадок колапсу.

Приймемо наступні обмеження:

дії факторів, що обумовлюють живучість, надійність, завадозахищеність і кіберзахищеність засобів кіберзахисту приймаємо як незалежними;

технічну надійність засобів кіберзахисту, на підставі робіт [9 – 15], що однозначно рекомендують приймати припущення, $P_{\text{ТН}} = 1$;

розрахунок потреб засобів кіберзахисту здійснюється окремо для однотипних груп засобів;

прогнозовані втрати засобів кіберзахисту є величина B_3 яку експертним методом призначають;

походження цінового (вартісного) показника одиниці засобу кіберзахисту береться за результатами щорічного моніторингу цін виробників необхідних засобів.

Методика розрахунку потреб ресурсного забезпечення об'єктів критичної інформаційної інфраструктури включає наступні етапи.

1. Розрахунок потреби організації у засобах кіберзахисту обчислюється за формулою (1):

$$P_z = N_z - N_z^f \quad (1)$$

де N_z – штатна чисельність засобів кіберзахисту;

N_z^f – фактично наявна чисельність засобів кіберзахисту;

P_z – потреба у засобах кіберзахисту.

Не вирішним до цього часу залишається об'єктивне визначення штатної чисельності засобів кіберзахисту (N_z). Дане завдання винесемо в перспективні напрямки подальших досліджень. На даний час пропонується визначати експертним методом.

2. Розрахунок потреби у засобах кіберзахисту на випадок колапсу. Обчислюється за формулою (2):

$$P_z^k = N_z^k - N_z^f - N_z^n \quad (2)$$

де N_z^k – штатна чисельність засобів кіберзахисту на випадок колапсу;

N_z^f – фактично наявна чисельність засобів кіберзахисту;

N_z^n – непорушний запас засобів кіберзахисту (обирається експертним методом);

P_z^k – потреба у засобах кіберзахисту на випадок колапсу.

3. Розрахунок остаточної потреби у засобах кіберзахисту на доукомплектування організації та відновлення на випадок колапсу здійснюється за формулою (3):

$$P_z^{ost} = P_z^k + V_z \quad (3)$$

де P_z^k – результат розрахунку штатної потреби на випадок колапсу (відповідно до етапу 2).

V_z – прогнозовані втрати засобів кіберзахисту у випадку колапсу;

P_z^{ost} – остаточна потреба у засобах кіберзахисту на доукомплектування та відновлення.

4. Розрахунок потреби у фінансовому резерві необхідного для закупівлі однотипних засобів в процесі доукомплектування та відновлення (остаточна) засобів кіберзахисту

4.1 Розрахунок потреби у фінансовому резерві необхідного для закупівлі однотипних засобів кіберзахисту в процесі доукомплектування та відновлення (остаточна) здійснюється за формулою (4):

$$F_{frz}^{ost} = P_z^{ost} \times C_z \quad (4)$$

де F_{frz}^{ost} – результат розрахунку фінансового резерву необхідного для закупівлі засобів кіберзахисту необхідного на доукомплектування та відновлення (остаточний);

C_z – ціна (вартість) однієї одиниці засобу кібернетичного захисту.

4.2 Розрахунок загальної потреби у фінансовому фонді для доукомплектування та відновлення засобів кіберзахисту здійснюється за формулою (5):

$$F_{fr} = \sum_{i=1}^{N} F_{frzi}^{ost} \quad (5)$$

де F_{fr} – остаточний результат розрахунку необхідного загального фінансового фонду для доукомплектування;

F_{frzi}^{ost} – результат розрахунку остаточного фінансового резерву необхідного для доукомплектування та відновлення груп однотипних засобів кіберзахисту.

5. Розрахунок потреби у штаті системних адміністраторів та обслуговуючого персоналу для обслуговування засобів кіберзахисту

5.1. Розрахунок потреби системних адміністраторів засобів кіберзахисту обчислюється за формулою (6):

$$P_{CA} = L_{CA} - L_{CA}^{f} \quad (6)$$

де L_{CA} – штатна чисельність системних адміністраторів засобів кіберзахисту;

L_{CA}^{f} – фактично наявна чисельність системних адміністраторів засобів кіберзахисту;

P_{CA} – потреба у системних адміністраторів засобах кіберзахисту.

5.2. Розрахунок потреби системних адміністраторів засобів кіберзахисту на випадок колапсу обчислюється за формулою (7):

$$P_{CA}^{k} = L_{CA}^{k} - L_{CA}^{f} - R_{CA} \quad (7)$$

де L_{CA}^{k} – штатна чисельність системних адміністраторів засобів кіберзахисту на випадок колапсу;

L_{CA}^{f} – фактично наявна чисельність системних адміністраторів засобів кіберзахисту;

R_{CA} – резерв (підсилення) системних адміністраторів засобів кіберзахисту;

P_{CA}^{k} – потреба у системних адміністраторах засобів кіберзахисту на випадок колапсу.

5.3. Розрахунок потреби обслуговуючого персоналу засобів кіберзахисту обчислюється за формулою (8):

$$P_{OP} = L_{OP} - L_{OP}^{f} \quad (8)$$

де L_{OP} – штатна чисельність обслуговуючого персоналу засобів кіберзахисту;

L_{OP}^{f} – фактично наявна чисельність обслуговуючого персоналу засобів кіберзахисту;

P_{OP} – потреба у обслуговуючому персоналі засобів кіберзахисту.

5.4. Розрахунок потреби обслуговуючого персоналу засобів кіберзахисту на випадок колапсу обчислюється за формулою (9):

$$P_{OP}^{k} = L_{OP}^{k} - L_{OP}^{f} - R_{OP} \quad (9)$$

де L_{OP}^{k} – штатна чисельність обслуговуючого персоналу засобів кіберзахисту на випадок колапсу;

L_{OP}^{f} – фактично наявна чисельність обслуговуючого персоналу засобів кіберзахисту;

R_{OP} – резерв (підсилення) обслуговуючого персоналу засобів кіберзахисту;

P_{OP}^{k} – потреба у обслуговуючому персоналі засобів кіберзахисту на випадок колапсу.

6. Розрахунок штатної чисельності та на випадок колапсу системних адміністраторів, обслуговуючого персоналу, який необхідний для обслуговування груп засобів кіберзахисту

6.1. Розрахунок штатної чисельності системних адміністраторів необхідних для обслуговування груп засобів кіберзахисту здійснюється за формулою (10):

$$L_{CA} = N_{gz} \times H_{gz(CA)} \quad (10)$$

де L_{CA} – результат розрахунку штатної чисельність системних адміністраторів необхідного для обслуговування всіх груп засобів кіберзахисту;

N_{gz} – кількість груп однотипних засобів кіберзахисту;

$H_{gz(CA)}$ – кількість системних адміністраторів необхідна для адміністрування групи однотипних засобів кіберзахисту.

6.2. Розрахунок штатної чисельності системних адміністраторів необхідних для обслуговування однотипних груп засобів кіберзахисту на випадок колапсу здійснюється за формулою (11):

$$L_{CA}^{k} = N_{gz} \times H_{gz(CA)} + R_{CA} \quad (11)$$

де L_{CA}^{k} – результат розрахунку штатної чисельності системних адміністраторів необхідних для обслуговування всіх груп однотипних засобів кіберзахисту на випадку колапсу;

R_{CA} – резерв (підсилення) системних адміністраторів засобів кіберзахисту.

6.3. Розрахунок штатної чисельності обслуговуючого персоналу необхідного для обслуговування однотипних груп засобів кіберзахисту інформації здійснюється за формулою (12):

$$L_{OP} = N_{gz} \times H_{gz(OP)} \quad (12)$$

де L_{OP} – результат розрахунку штатної чисельності обслуговуючого персоналу необхідного для обслуговування всіх груп однотипних засобів кіберзахисту;

$H_{gz(OP)}$ – кількість обслуговуючого персоналу необхідного для обслуговування групи однотипних засобів кіберзахисту.

6.4. Розрахунок штатної чисельності (випадок колапсу) обслуговуючого персоналу необхідного для обслуговування груп засобів кіберзахисту здійснюється за формулою (13):

$$L_{OP}^{k} = N_{gz} \times H_{gz(OP)} + R_{OP} \quad (13)$$

де L_{OP}^{k} – результат розрахунку штатної чисельність обслуговуючого персоналу необхідного для обслуговування всіх груп однотипних засобів кіберзахисту на випадок колапсу;

R_{OP} – резерв (підсилення) обслуговуючого персоналу для обслуговування засобів кіберзахисту.

7. Розрахунок коефіцієнта укомплектованості засобів кіберзахисту.

7.1. Розрахунок коефіцієнта укомплектованості засобами кіберзахисту пропонується обчислювати за формулою (14):

$$K_{uz} = \frac{N_{z}^{f}}{N_{z}} \quad (14)$$

де K_{uz} – коефіцієнт укомплектованості засобами кіберзахисту;

N_z – штатна чисельність засобів кіберзахисту;

N_z^f – фактично наявна чисельність засобів кіберзахисту.

7.2. Розрахунок коефіцієнта укомплектованості засобів кіберзахисту на випадок колапсу пропонується обчислювати за формулою (15):

$$K_{uz}^k = \frac{N_z^f}{N_z^k} \quad (15)$$

де K_{uz}^k – коефіцієнт укомплектованості засобів кіберзахисту на випадок колапсу;

N_z^k – штатна чисельність засобів кіберзахисту на випадок колапсу;

N_z^f – фактично наявна чисельність засобів кіберзахисту.

7.3. Розрахунок коефіцієнта технічної готовності засобів кіберзахисту здійснюється за формулою (16):

$$K_{tgz} = \frac{N_z^s}{N_z^f} \quad (16)$$

де K_{tgz} – коефіцієнт технічної готовності засобів кіберзахисту;

N_z^s – кількість справних засобів кіберзахисту;

N_z^f – фактично наявна чисельність засобів кіберзахисту.

7.4. Розрахунок коефіцієнта технічної готовності засобів кіберзахисту на випадок колапсу пропонується обчислювати за формулою (17):

$$K_{tgz}^k = \frac{N_z^s}{N_z^f} \quad (17)$$

де K_{tgz}^k – коефіцієнт технічної готовності засобів кіберзахисту на випадок колапсу;

N_z^s – кількість справних засобів кіберзахисту на випадок колапсу; K_{usz}^k

N_z^f – фактично наявна чисельність засобів кіберзахисту на випадок колапсу.

7.5. Розрахунок коефіцієнта укомплектованості справними засобами кіберзахисту пропонується обчислювати за формулою (18):

$$K_{usz} = K_{uz} \times K_{tgz} = \frac{N_z^s}{N_z} \quad (18)$$

де K_{usz} – коефіцієнт укомплектованості справними засобами кіберзахисту;

K_{uz} – коефіцієнт укомплектованості засобів кіберзахисту;

K_{tgz} – коефіцієнт технічної готовності засобів кіберзахисту;

N_z^s – кількість справних засобів кіберзахисту;

N_z – штатна чисельність засобів кібернетичного захисту.

7.6. Розрахунок коефіцієнта укомплектованості справними засобами кіберзахисту на випадок колапсу пропонується обчислювати за формулою (19):

$$K_{usz}^k = K_{uz}^k \times K_{tgz}^k = \frac{N_z^s}{N_z^k} \quad (19)$$

де K_{usz}^k – коефіцієнт укомплектованості справними засобами кіберзахисту на випадок колапсу;

K_{uz}^k – коефіцієнт укомплектованості засобів кіберзахисту на випадок колапсу;

K_{tgz}^k – коефіцієнт технічної готовності засобів кіберзахисту на випадок колапсу;

N_z^s – кількість справних засобів кіберзахисту;

N_z^k – штатна чисельність засобів кіберзахисту на випадок колапсу.

8. Оцінювання за критерієм спроможності організації виконувати завдання за призначенням в штатному режимі та у випадку колапсу.

Критерії спроможності організації виконувати завдання за призначенням в штатному режимі та у випадку колапсу наведені в табл. 1.

Таблиця 1

Критерії спроможності організації виконувати завдання за призначенням в штатному режимі та у випадку колапсу

Показник	Критерій	Рівень	Лінгвістичний опис
K_{usz}	$0{,}75 < K_{usz} \le 1$	Високий	ОКІІ не доукомплектований за штатного режиму, але готовий до кіберзахисту
	$0{,}5 < K_{usz} \le 0{,}75$	Середній	ОКІІ не укомплектований за штатного режиму, обмежено готовий до кіберзахисту
	$0 \le K_{usz} \le 0{,}5$	Низький	ОКІІ не готовий до кіберзахисту
K_{usz}^k	$0{,}75 < K_{usz}^k \le 1$	Високий	ОКІІ не доукомплектований за штатного режиму, але готовий до кіберзахисту
	$0{,}5 < K_{usz}^k \le 0{,}75$	Середній	ОКІІ не укомплектований за штатного режиму, обмежено готовий до кіберзахисту
	$0 \le K_{usz}^k \le 0{,}5$	Низький	ОКІІ не готовий до кіберзахисту

Висновки й перспективи подальших досліджень

В науковій статті подано рішення наукового завдання з розробки методики планування потреби в забезпечення виконання заходів кібербезпеки ОКІІ. Методика націлена підвищити ефективність функціонування системи кібербезпеки ОКІІ за рахунок своєчасного планування потреби в забезпеченні виконання заходів кібербезпеки ОКІІ з урахуванням колапсу інформаційно-телекомунікаційних систем.

Проблемним і не вирішеним до цього часу лишається питанням об'єктивного визначення штатної чисельності засобів кіберзахисту. Тому пропонується його пошук (обґрунтування) визначити як перспективним напрямком подальших наукових досліджень.

Вперше запропоновано методику розрахунку потреб ресурсного забезпечення об'єктів критичної інформаційної інфраструктури. Методика забезпечує можливість відповідальний особі у структурно-відокремлених підрозділах ОКІІ за єдиним шаблоном розраховувати потреби ресурсного забезпечення.

Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні та практичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого її вивчення та уточнення.

Література

1. Слипченко В.И. Войны шестого поколения оружие и военное искусство будущего. М.: Вече, 2002. 382 с. **2. Петренко А.Г.** План дій щодо впровадження оборонної реформи у 2016-2020 роках (дорожня карта оборонної реформи). К.: ДВПСП та МС МО України, 2016. 210 с. **3. Козубцов І.М., Козубцова Л.М., Терещенко Т.П., Куцаєв В.В.** Глобальний колапс інформаційно-телекомунікаційних систем в наслідок порушення роботи сучасних інформаційних технологій у секторі безпеки і оборони. «*Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи*» Міжнародна науково-практична конференція (Одеса, 12-13 вересня 2019 р.). Військова академія, 2019. С. 229–230. **4. Козубцов І.М., Козубцова Л.М.** Прогноз можливих наслідків настання "колапсу інформаційних систем спеціального призначення". *Актуальні проблеми управління інформаційною безпекою держави*: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). Київ: НА СБУ, 2021. С. 50–53. **5.** Рішення Ради національної безпеки і оборони України від 10.07.17 "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року" "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації", введеного в дію Указом Президента України від 13.02.17 №254/2017. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17
6. Лобода Ю.О. Поняття «гібридна війна (гібридні військові дії)»: походження та складність. Журнал «*Наука і оборона*». 2020. С. 20–23. **7. Грицюк Ю.І.** Особливості реалізації принципу розумної достатності функціонування комплексної системи захисту інформації на підприємстві. *Науковий вісник НЛТУ України*. 2015. Вип. 25.4. С. 313–324. **8. Шубинский И.Б.** Структурная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 216 с. **9. Гончар С.Ф., Герасимов Р.П., Ткаченко В.В.** Дослідження проблеми кіберживучості Об'єднаної енергосистеми України. Міжнародний науково-теоретичний журнал "*Електронне моделювання*". 2019. Т.41. №1. С. 43–54. **10. Захарченко Р.И., Королев И.Д.** Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве. *Наукоемкие технологии в космических исследованиях Земли*. 2018. Т.10. №2. С. 52–61. **11. Минаев В.А., Королев И.Д., Зеленцова Е.В., Захарченко Р.И.** Критическая информационная инфраструктура: оценка устойчивости функционирования. *Радиопромышленность*. 2018. Т. 28. №4. С. 59–67. **12. Минаев В.А., Крупенин А.В., Королев И.Д., Бондарь К.М., Захарченко Р.И.** Оценка устойчивости функционирования критической информационной инфраструктуры. *Вестник РосНОУ, серия «Сложные системы: модели, анализ и управление»*. 2018. Вып. 4. Информатика и вычислительная техника. С. 129–138. **13.Козубцов І.М., Хлапонін Ю.І., Козубцова Л.М.** Ідея впровадження зворотного зв'язку як вдосконалення функціональної залежності реалізації кібернетичної безпеки. *"Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку*" Міжнародна науково-практична конференція (Харків, 15 березня 2021 р.). Харків. НАНГ України, 2021. С. 86–87.

МЕТОДИКА РАСЧЕТА ПОТРЕБНОСТЕЙ РЕСУРСНОГО ОБЕСПЕЧЕНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

***Леся Михайловна Козубцова** (кандидат технических наук)[1]*
***Владимир Николаевич Подоляк** (кандидат технических наук, доцент)[2]*
***Игорь Николаевич Козубцов** (доктор педагогических наук, старший научный сотрудник)[1]*

[1]Военный институт телекоммуникаций и информатизации имени Героев Крут, Киев, Украина
[2] Луцкий национальный технический университет, Луцк, Украина

В научной статье впервые предложена методика расчета потребностей ресурсного обеспечения объектов критической информационной инфраструктуры. Под "потребностью в обеспечении выполнения мер кибербезопасности объектов критической информационной инфраструктуры" в статье предложена следующая формулировка: как необходимое количество средств киберзащиты и обслуживающего персонала для обеспечения надлежащего функционирования этой системы. Потребность в разработке этой методики возникла в результате анализа последних исследований и

публикаций показал отсутствие в открытом доступе аналогичной методики. Указанная методика необходима владельцу объекта критической информационной инфраструктуры для своевременного планирования ресурсного обеспечения объектов критической информационной инфраструктуры. Эти данные также необходимы для обеспечения эффективного функционирования объекта критической информационной инфраструктуры, а, следовательно, выполнять свою целевую функцию. Методика включает следующие ключевые этапы расчета, а именно: потребности организации в средств киберзащиты; потребности в средствах киберзащиты на случай коллапса; окончательной потребности в средствах киберзащиты на доукомплектование организации и восстановления на случай коллапса; потребности в финансовом резерве необходимого для закупки однотипных средств в процессе доукомплектования и восстановления (окончательная) средств киберзащиты; потребности в штате системных администраторов и обслуживающего персонала для обслуживания средств киберзащиты; штатной численности (и на случай коллапса) системных администраторов и обслуживающего персонала необходимого для обслуживания групп средств киберзащиты; коэффициента укомплектованности средств киберзащиты. Данная статья является результатом продолжением исследования в направлении "Будущая безопасность среды 2030". Результат расширяет научные границы по реализации неотложных мер государственной политики по нейтрализации угроз кибербезопасности объектов критической информационной инфраструктуры. Научная новизна. Впервые разработана методика расчета потребностей ресурсного обеспечения объектов критической информационной инфраструктуры. Методика обеспечивает возможность ответственному лицу в структурно-обособленных подразделениях объектов критической информационной инфраструктуры по единому шаблону рассчитывать потребности ресурсного обеспечения.

Ключевые слова: *методика, расчет, потребности, ресурс, обеспечение, кибербезопасность, объект критической информационной инфраструктуры.*

METHODOLOGY FOR CALCULATING THE RESOURCE NEEDS OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Lesja Kozubtsova *(Candidate of Technical Sciences)*[1]
Volodymyr Podolyak *(Candidate of Technical, Associate Professor)*[2]
Igor Kozubtsov *(Doctor of Pedagogical Sciences, Senior Research Fellow)*[1]

[1] ***Military Institute of Telecommunications and Informatization named after Heroes of Kruty Kyiv, Ukraine***
[2] ***Lutsk National Technical University, Lutsk, Ukraine***

The scientific article for the first time offers a method for calculating the resource requirements of critical information infrastructure facilities. Under the "need to ensure the implementation of cybersecurity measures for critical information infrastructure facilities", the following wording is proposed in the article: as the necessary amount of cyber defense and maintenance personnel to ensure the proper functioning of this system. The need to develop this methodology arose as a result of the analysis of recent studies and publications showed the absence of a similar methodology in the public domain. This technique is necessary for the owner of a critical information infrastructure facility for timely resource planning of critical information infrastructure facilities. These data are also necessary to ensure the effective functioning of the critical information infrastructure object, and, consequently, to fulfill its target function. The methodology includes the following key stages of calculation, namely: the needs of the organization for cyber defense means; the needs for cyber defense means in case of collapse; the final need for cyber defense equipment for the organization's staffing and recovery in case of collapse; the need for a financial reserve necessary for the purchase of the same type of funds in the process of completing and restoring (final) cyber defense equipment; the need for the staff of system administrators and maintenance personnel for the maintenance of cyber defense equipment; staffing levels (and in case of collapse) of system administrators and maintenance personnel necessary for the maintenance of groups of cyber defense equipment; the staffing ratio of cyber defense equipment. This article is the result of a continuation of the research in the direction of "Future security of the environment 2030". The result expands the scientific boundaries for the implementation of urgent state policy measures to neutralize threats to the cybersecurity of critical information infrastructure facilities. Scientific novelty. For the first time, a methodology for calculating the resource requirements of critical information infrastructure facilities has been developed. The methodology provides an opportunity for the responsible person in structurally separate subdivisions of critical information infrastructure facilities to calculate resource requirements according to a single template.

Keywords*: methodology, calculation, needs, resource, provision, cybersecurity, object of critical information infrastructure.*

References

1. Slipchenko V.I. (2002) Wars of the sixth generation are weapons and military art of the future [Voynyi shestogo pokoleniya oruzhie i voennoe iskusstvo buduschego] Moscow: Veche. 382 p. **2. Petrenko A.H.** (2016) Action plan for the implementation of defense reform in 2016-2020 (road map of defense reform) [Plan dii shchodo vprovadzhennia oboronnoi reformy u 2016-2020 rokakh (dorozhnia karta oboronnoi reformy)]. K.: DVPSP ta MS MO Ukrainy, 210 p. **3. Kozubtsov I.M.,** Kozubtsova L.M., Tereshchenko T.P., Kutsaiev V.V. (2019) Global collapse of information and telecommunications systems as a result of disruption of modern information technologies in the security and defense sector [Hlobalnyi kolaps informatsiino-telekomunikatsiinykh system v naslidok porushennia roboty suchasnykh informatsiinykh tekhnolohii u sektori bezpeky i oborony] International scientific and practical conference "joint actions of military formations and law enforcement agencies of the state: problems and prospects" (Odessa, September 12-13, 2019). Military Academy. Pp.229–230. **4. Kozubtsov I.M.,** Kozubtsova L.M. (2021) Forecast of possible consequences of the "collapse of special purpose information systems" [Prohnoz mozhlyvykh naslidkiv nastannia “kolapsu informatsiinykh system spetsialnoho pryznachennia”]. Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy: zb. tez nauk. dop. nauk.-prakt. konf. (Kyiv, 26 bereznia 2021). Kyiv: NA SBU. Pp.50–53. **5.** Decision of the National Security and Defense Council of Ukraine dated 10.07.17 "On the status of implementation of the decision of the National Security and Defense Council of Ukraine dated December 29, 2016" "On threats to cybersecurity and urgent measures to neutralize them", enacted by Presidential Decree of 13.02.17 №254/2017. [Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 10.07.17 “Pro stan vykonannia rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku” “Pro zahrozy kiberbezpetsi derzhavy ta nevidkladni zakhody z yikh neitralizatsii”, vvedenoho v diiu Ukazom Prezydenta Ukrainy vid 13.02.17 №254/2017]. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17. **6. Loboda Yu.**O. (2020) The concept of "hybrid war (hybrid military actions)": origin and complexity [Poniattia «hibrydna viina (hibrydni viiskovi dii)»: pokhodzhennia ta skladnist] Journal "Science and defense". Pp. 20–23. **7. Hrytsiuk Yu.I.** (2015) Features of implementation of the principle of reasonable sufficiency of functioning of the integrated information security system at the enterprise [Osoblyvosti realizatsii pryntsypu rozumnoi dostatnosti funktsionuvannia kompleksnoi systemy zakhystu informatsii na pidpryiemstvi] Scientific Bulletin of NLTU of Ukraine. Issue 25.4. Pp. 313–324. **8. Shubinskiy I.B.** (2012) Structural reliability of information systems. Methods of analysis [Strukturnaya nadezhnost informatsionnyih sistem. Metodyi analiza] M.: Journal Reliability. 216 p. **9. Honchar S.F**., Herasymov R.P., Tkachenko V.V. (2019) Research of the problem of cyber consumption of the United energy system of Ukraine [Doslidzhennia problemy kiberzhyvuchosti Obiednanoi enerhosystemy Ukrainy] International scientific and theoretical journal “Electronic modeling”. Vol.41. №1. Pp. 43–54. **10. Zaharchenko R.I.,** Korolev I.D. (2018) Methodology for assessing the sustainability of the functioning of critical information infrastructure objects operating in cyberspace [Metodika otsenki ustoychivosti funktsionirovaniya ob'ektov kriticheskoy informatsionnoy infrastrukturyi funktsioniruyuschey v kiberprostranstve]. Naukoemkie tehnologii v kosmicheskih issledovaniyah Zemli. Vol.10. No.2. Pp.52–61. **11. Minaev V.A.,** Korolev I.D., Zelentsova E.V., Zaharchenko R.I. (2018) Critical information infrastructure: assessment of the stability of functioning [Kriticheskaya informatsionnaya infrastruktura: otsenka ustoychivosti funktsionirovaniya] Radio industry. Vol.28. No.4. Pp. 59–67. **12. Minaev V.A.,** Krupenin A.V., Korolev I.D., Bondar K.M., Zaharchenko R.I. (2018) Assessment of the stability of the functioning of critical information infrastructure [Otsenka ustoychivosti funktsionirovaniya kriticheskoy informatsionnoy infrastrukturyi] Bulletin of RosNOU, series "Complex systems: models, analysis and management". Issue 4. Computer Science and Computer engineering. Pp. 129–138. **13. Kozubtsov I.M**., Khlaponin Yu.I., Kozubtsova L.M. (2021) The idea of introducing feedback as improving the functional dependence of cybernetic security implementation [Ideia vprovadzhennia zvorotnoho zviazku yak vdoskonalennia funktsionalnoi zalezhnosti realizatsii kibernetychnoi bezpeky] International scientific and practical conference “application of information technologies in the training and activities of law enforcement forces” (Kharkiv, March 15, 2021). Kharkiv. Nang of Ukraine. Pp. 86–87.