УДК 004.8:004.912

Леонід Михайлович Артюшин *(доктор техн. наук, професор)*[1]
Сергій Вікторович Чернишук *(канд. техн. наук)*[2]

[1] ***Державний науково-дослідний інститут авіації, Київ, Україна***
[2] ***Житомирський військовий інститут ім. С. П. Корольова, Житомир, Україна***

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ВИЯВЛЕННЯ ТА ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ

У статті розглянуто типовий порядок організації та ведення моніторингу відкритих джерел інформації спеціальними підрозділами Збройних Сил України в інтересах виявлення та оцінювання рівня інформаційних загроз. Проаналізовано існуючі підходи до виявлення та оцінювання рівня інформаційних загроз, встановлено їх переваги і недоліки, визначено показники, часові та ресурсні обмеження щодо такого виду діяльності у Збройних Силах України. Сформульовано та формалізовано задачу підвищення ефективності виявлення й оцінювання рівня інформаційних загроз.

На рівні функціонування засобів моніторингу відкритих джерел інформації запропоновано шляхи підвищення ефективності системи виявлення та оцінювання рівня інформаційних загроз. Зокрема, розроблено механізм раціонального використання обмеженої кількості таких засобів, що передбачає узгодження їх роботи шляхом об'єднання в єдину цілісну систему, здатну до адаптивного реконфігурування для найкращого пристосування до зміни умов застосування. Для цього розв'язано задачу синтезу системи виявлення інформаційних загроз за результатами моніторингу відкритих джерел інформації. Розв'язок такої задачі виконано в три етапи: визначено призначення, функції та склад системи; визначено кількісний та якісний склад компонентів системи й обґрунтовано їх параметри; виконано адаптивний перерозподіл наявних технічних засобів з урахуванням зміни навантаження на компоненти системи.

Ключові слова: *інформаційні загрози, відкриті джерела інформації, підвищення ефективності, Збройні Сили України.*

Вступ

Стійка тенденція останніх років до перенесення протиборства в інформаційне середовище привела до зростання ролі інформаційних загроз (ІЗ) у забезпеченні безпеки держави у воєнній сфері [**Ошибка! Источник ссылки не найден.**]. Стрімке збільшення кількості таких загроз та постійне підвищення рівня їх небезпеки [0–4] спричинило виникнення актуального наукового завдання, що полягає у підвищенні як оперативності виявлення ІЗ, так і достовірності оцінювання рівня їх небезпеки з метою своєчасного реагування і протидії.

Постановка проблеми. Окремі завдання з виявлення та оцінювання ІЗ у воєнній сфері за результатами моніторингу відкритих джерел інформації (ВДІ) покладено на спеціальні підрозділи Збройних Сил (ЗС) України [5, 6]. Зразки озброєння і військової техніки, якими укомплектовані зазначені підрозділи, а також їх науково-методичне забезпечення на сьогодні мають суттєво обмежені можливості і вже не відповідають потребам військ у повній мірі. Крім того, недостатність та розрізненість сил і засобів, виділених для ведення моніторингу ВДІ, недостатній рівень автоматизації, недосконалі алгоритми обробки та суб'єктивні методи аналізу добутих матеріалів на наявність ознак ІЗ в умовах постійного зростання кількості ВДІ та підвищення інтенсивності інформаційних потоків, які у них циркулюють, призводять до зниження ефективності виконання спеціальними підрозділами ЗС України завдань за призначенням.

Аналіз остатніх досліджень і публікацій. Дослідженню проблем забезпечення інформаційної безпеки, виявлення та оцінювання рівня ІЗ, своєчасного та адекватного реагування на їх прояви присвячено роботи багатьох вчених, зокрема О. В. Левченка [3, 7], В. П. Горбуліна [8], Р. В. Грищука [4], В. Л. Бурячка [9], О. Г. Корченка [10], В. О. Хорошка [11], D. Ventre [0] та ін. Утім аналіз зазначених та схожих за проблематикою робіт показав, що для автоматизованого (автоматичного) пошуку ознак ІЗ аналізуються здебільшого показники технічних датчиків, програмний код та метричні характеристики роботи складових інформаційних систем (користувачів, програм, процесів) [8, 9], а використання потенціалу ВДІ, які на даний час характеризуються повнотою розміщених даних та оперативністю їх оновлення [9], досить обмежено. Як наслідок, втрачається можливість завчасного виявлення ІЗ та знижується достовірність оцінювання їх рівня. Тому надалі, окрім зазначеного вище, актуальним залишається завдання раціонального використання обмежених сил і засобів шляхом синтезу оптимальних за структурою і параметрами систем. Саме її вирішення і виступатиме підґрунтям для

розроблення нових систем виявлення із урахуванням сучасних особливостей моніторингу ВДІ, які проявляються у високій інтенсивності надходження вхідних інформаційних потоків та динамічній зміні навантаження на компоненти системи воєнної моніторингу України.

Мета статті. Отже, існує протиріччя між постійно зростаючою кількістю ВДІ за відсутності прийнятних підходів до раціонального використання обмежених сил і засобів, виділених у підрозділах ЗС України для моніторингу таких джерел, та потребою в ефективному виявленні та оцінюванні рівня ІЗ з причини недосконалості науково-методичного забезпечення відповідних засобів автоматизації.

Метою роботи є підвищення ефективності системи виявлення та оцінювання рівня небезпеки ІЗ за результатами моніторингу ВДІ в умовах часових і ресурсних обмежень спеціальних підрозділів ЗС України.

Виклад основного матеріалу дослідження.

На підставі проведеного науково-технічного аналізу встановлено, що з позицій ефективного виявлення та оцінювання рівня ІЗ для своєчасного прийняття правильного рішення на протидію необхідно забезпечити максимальну повноту охоплення ВДІ, оперативне і точне виявлення ознак ІЗ, достовірне оцінювання рівня їх небезпеки в умовах зростаючого інформаційного потоку при часових і ресурсних обмеженнях. Для цього у провідних країнах світу й у ЗС України використовуються спеціальні автоматизовані системи моніторингу ВДІ, побудову яких слід розглядати з погляду трьох рівнів: технічного, науково-методичного та організаційного [4, 13–15].

Організаційний рівень розгорнутих у підрозділах ЗС України систем моніторингу ВДІ, що, зокрема, включає організаційно-штатні заходи та кадрове забезпечення, у подальшому не розглядається, оскільки не належить до сфери компетенції авторів.

Науково-методичне забезпечення системи моніторингу ВДІ в інтересах виявлення ІЗ включає методи і моделі автоматичної обробки текстової інформації, а також механізми виявлення та оцінювання рівня ІЗ. На даний час апарат автоматичної обробки текстів достатньо опрацьований і дозволяє успішно вирішувати завдання аналізу великих об'ємів інформації [11]. Науково-методичне забезпечення виявлення ІЗ у переважній більшості ґрунтується на апараті теорії розпізнавання образів, застосування якого до даних моніторингу ВДІ потребує формування переліку семантичних ознак загрози та критеріїв їх аналізу, що неможливо здійснити для нових ІЗ, апріорна інформація про які відсутня [4, 11]. Оцінювання рівня ІЗ TL здійснюється за виразом (1) з урахуванням імовірності реалізації загрози PR, величини нанесеного збитку DC та ефективності заходів протидії CM:

$$TL = PR \cdot DC - CM. \quad (1)$$

Розрахунок величин PR і CM у виразі (1) здійснюється, як правило, методами експертного та статистичного оцінювання. У першому випадку не забезпечується достатня об'єктивність результатів оцінювання, у другому – тривалого накопичення потребують статистичні характеристики проявів ІЗ, що не завжди можливо через відсутність достатніх апріорних даних про загрозу. Разом з тим, у проаналізованих підходах при оцінюванні рівня небезпеки ІЗ не враховується структурна уразливість інформаційної системи, для якої виявлено загрози. Як наслідок, зростає складність процесу оцінювання та знижується достовірність його результатів, що не дозволяє своєчасно та адекватно реагувати на зміну рівня небезпеки ІЗ. Удосконалення науково-методичного забезпечення систем моніторингу ВДІ потребує окремих ґрунтовних досліджень, які передбачається виконати у подальшому.

Технічний рівень систем моніторингу ВДІ становлять окремі автоматизовані робочі місця (АРМ) [12, 13], потенціал об'єднання яких в єдину систему моніторингу залишається не використаним. Для його реалізації необхідно розробити механізм синтезу розрізнених робочих місць у цілісну систему та її реконфігурування залежно від умов обстановки.

З наведеного вище задача підвищення ефективності виявлення й оцінювання рівня ІЗ може бути сформульована таким чином: для підвищення ефективності E системи виявлення та оцінювання рівня ІЗ необхідно забезпечити опрацювання максимальної кількості ВДІ F, виявлення ознак ІЗ у змісті ПМТ за мінімальний час T з максимальною точністю A в умовах високої інтенсивності інформаційного потоку ($N \approx 20 \cdot 10^3$ пов./доба) при часових ($T \le T_{доп.}$) і ресурсних ($B \le B_{вид.}$) обмеженнях підрозділів ЗС України за виділеними силами і засобами, а також оцінювання рівня небезпеки виявлених загроз з максимальною достовірністю D в умовах відсутності апріорної інформації про загрози $I_{апр.} < I_{необх.}$:

$$\begin{cases} E = \Phi(F, T, A, D) \to \max \\ F \to \max, \ F \ge N \text{ при } N \approx 20 \cdot 10^3, B \le B_{вид.}, \\ T \to \min, \ T \le T_{доп.} \text{ при } T_{доп.} \le 5 \text{ с}, \\ A \to \max, \ A \ge A_{доп.}, \\ D \to \max \text{ при } I_{апр.} < I_{необх.}. \end{cases} \quad (2)$$

Для підвищення повноти охоплення ВДІ F за рахунок раціонального використання виділених сил і засобів пропонується на рівні технічного забезпечення систем виявлення та оцінювання ІЗ

розробити механізм раціонального використання обмеженої кількості АРМ, які різняться між собою за можливостями та характеристиками. Для цього слід забезпечити узгодження їх роботи шляхом об'єднання в єдину цілісну систему, здатну до адаптивного реконфігурування для найкращого пристосування до зміни умов застосування. З цією метою розв'язано задачу синтезу системи виявлення ІЗ за результатами моніторингу ВДІ з визначенням її структури та параметрів.

Розв'язок такої задачі здійснено за три етапи, що передбачають: структуризацію системи із застосуванням евристичного методу для визначення її складу, призначення та функцій; визначення кількісного та якісного складу компонентів системи з подальшим обґрунтуванням їх параметрів на основі оптимізаційних методів; адаптивний перерозподіл наявних АРМ з урахуванням зміни навантаження на компоненти системи.

На першому етапі на підставі результатів аналізу архітектури існуючих систем виявлення ІЗ за результатами моніторингу ВДІ та узагальнення відомих підходів до їх побудови у структурі системи, що синтезується, запропоновано виділяти такі взаємопов'язані укрупнені компоненти, наведені у порядку пріоритету (рис. 1): пошуку (ПсП); спостереження (ПсС); ідентифікації та оцінювання ІЗ (ПсІО). Кожному із зазначених компонентів поставлено у відповідність скінченне число часткових функцій системи FS_i.

Синтез системи на стадії її впровадження здійснюється шляхом розподілу обмеженої кількості наявних АРМ з формулярами ARM_j за компонентами системи з формулярами FS_i при виконанні конфліктних вимог мінімізації часу на добування та обробку необхідних даних ($T_s \to \min$) і максимізації повноти охоплення ВДІ ($F_s \to \max$).

Регуляризацію некоректної оптимізаційної задачі з конфліктними критерійними вимогами здійснено методами багатокритерійного аналізу шляхом переходу до однокритерійної форми. Формування узагальненого критерію оптимальності реалізовано з використанням нелінійної схеми компромісів відповідно до згортки [15]. У результаті отримано багатокритерійну оптимізаційну математичну модель (3) структурно-параметричного синтезу системи, що становить зміст другого етапу розв'язку задачі:

Рис. 1. Функціональна структура системи виявлення ІЗ за результатами моніторингу ВДІ

$$\Psi_i^j = KS_{i0}^j \left(1 - S_{i0}^j\right)^{-1} + KTX_{j0}\left(1 - TX_{j0}\right)^{-1} \qquad (3)$$

де $S_i^j = [FS_i \times FA_j]$ – відображення формуляра i-го компонента на формуляри j-го АРМ;

$KS_j^i = [S_i^j \times N_{kod}]$ – відображення S_i^j на двійковий код N_{kod};

TX_j – технічні обмеження, які залежать від характеристик програмних й апаратних засобів j-го АРМ;

$KTX_j = [TX_j \times N_{kod}]$ – відображення TX_j на двійковий код N_{kod};

$N_{kod} = \begin{Bmatrix} N_{kod\,1} & N_{kod\,2} & N_{kod\,3} \\ 2^0 & 2^1 & 2^2 \end{Bmatrix}, \ldots$ – двійковий код числа; нижнім індексом 0 позначено нормовані значення складових виразу (3).

Вибір конкретного АРМ із числа доступних для формування структури системи реалізується шляхом контролю виконання вимоги мінімізації значень $\Psi_i^j \to \min$ для кожного j-го АРМ. Подальший розподіл АРМ за компонентами системи здійснюється за спеціальним алгоритмом із урахуванням пріоритетності відповідних компонентів для функціонування системи в цілому.

На третьому етапі запропоновано алгоритм адаптивного реконфігурування синтезованої системи (рис. 2) для своєчасного реагування у разі зміни навантаження на її компоненти в процесі моніторингу ВДІ (зростання або зниження інтенсивності інформаційних потоків, пошукових завдань тощо), який передбачає: формування повного переліку $VK_N(t)$ можливих конфігурацій системи на підставі оптимізаційної моделі (3); перерахунок для всіх конфігурацій узагальненого показника відповідності i-ї підсистеми $\Psi_i'^{(n)} = \beta_i(t)\sum_{j=1}^{d}\Psi_i^j$ своєму призначенню із урахуванням зміни навантаження $\lambda_i(t) = \beta_i\lambda_i^*$ ($\beta_i \in (0,\infty)$); вибір оптимальної конфігурації $F^*(t)$ за мінімальним значенням цільової функції ефективності роботи всієї системи

$$F_n = \sum_{n=1}^{N}\Psi_i'^{(n)} \to \min.$$

У сукупності зазначені етапи дають можливість проводити структурно-параметричний синтез системи виявлення ІЗ за результатами моніторингу ВДІ, який дозволяє на стадії впровадження системи оптимальним чином розподілити наявні

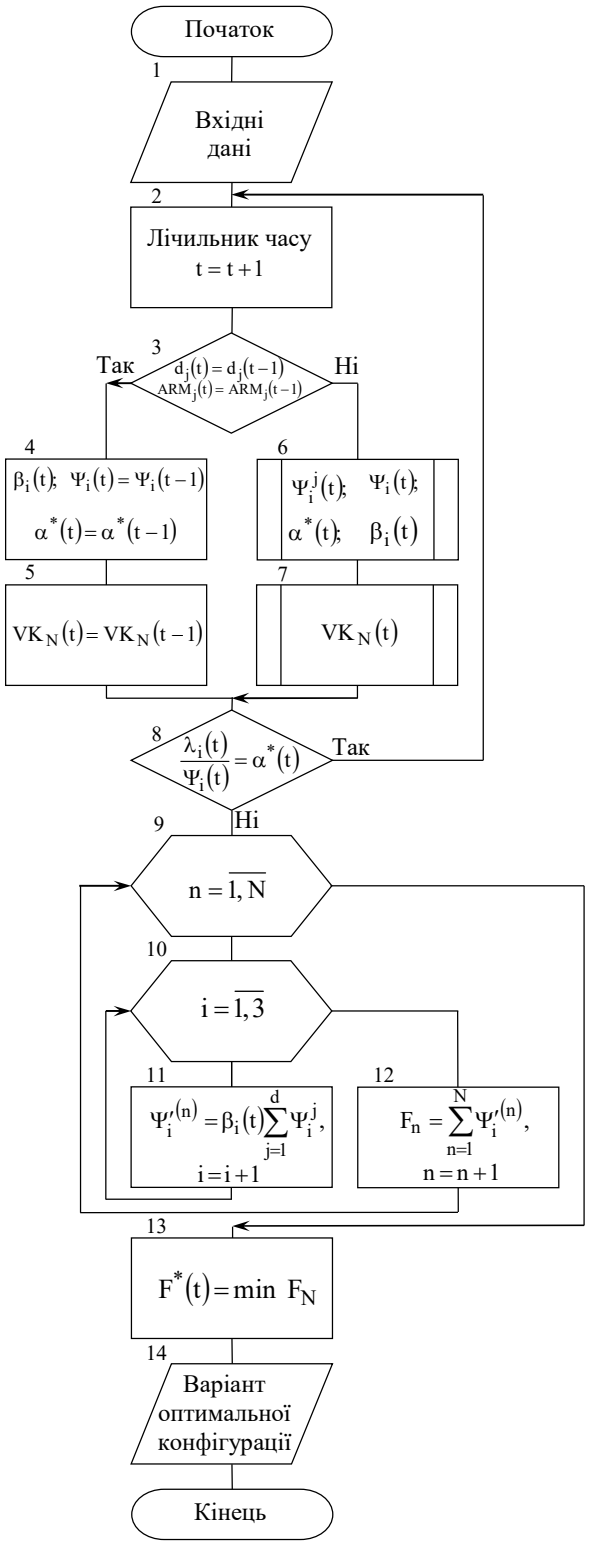

Рис. 2. Алгоритм адаптивного реконфігурування системи

АРМ за її компонентами, а на стадії експлуатації – реконфігурувати систему із урахуванням динамічної зміни навантаження на її компоненти.

Оцінювання ефективності застосування запропонованого механізму синтезу системи виявлення ІЗ за результатами моніторингу ВДІ проведено шляхом експериментальної перевірки, яка здійснювалася за два етапи:

на стадії впровадження системи оцінено

ефективність застосування оптимізаційної моделі (3) шляхом порівняння показників ефективності функціонування системи у разі розрізнених АРМ та їх об'єднання в єдину систему;

на стадії експлуатації системи визначено ефективність застосування алгоритму адаптивного реконфігурування.

Результати застосування моделі (3) для синтезу системи із 10 АРМ, які можуть бути залучені у спеціальному підрозділі ЗС України для виконання відповідних завдань, свідчать про зростання повноти охоплення ВДІ F на стадії впровадження системи в середньому у 1,5 рази (табл. 1).

Таблиця 1 – Результати синтезу системи на етапі впровадження

Показники ефективності	Варіант застосування засобів	
	Розрізнені засоби	Синтезована система
Повнота охоплення ВДІ F, пов./зміна	640	**960**
Середня продуктивність $\bar{\mu}$ одного АРМ, пов./зміна	64,0	**96,0**

Виходячи з припущення про те, що середня продуктивність АРМ $\bar{\mu}$ не змінюється протягом доби, побудовано графік залежності $F(B) = 3\mu B$ (рис. 3), за яким встановлено, що прийнятне значення повноти охоплення ВДІ F (2) не забезпечується у межах наявних у спеціальних підрозділах ЗС України засобів моніторингу ΔB.

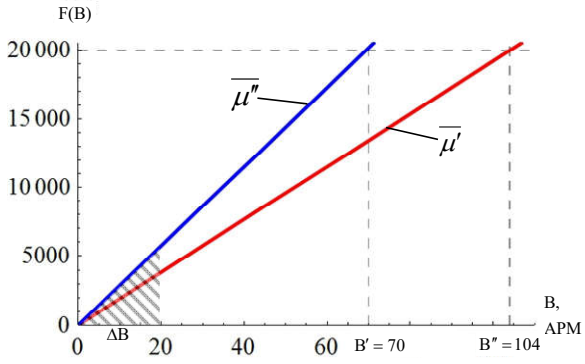

Рис. 3. Залежність повноти охоплення ВДІ від кількості засобів моніторингу

Результати застосування алгоритму адаптивного реконфігурування системи на стадії її експлуатації наведено у табл. 2.

Отримані дані свідчать про адекватність алгоритму, що підтверджується пропорційною зміною кількісного складу $B_{сп.}$ компонентів системи виявлення ІЗ за результатами моніторингу ВДІ при зміні навантаження на її підсистеми. Як наслідок, у період надходження найбільш інтенсивного інформаційного потоку (з 10.00 до 20.00 години) повнота охоплення ВДІ зросла у 1,8 рази, а загальна повнота охоплення системою ВДІ за добу – у 1,3 рази.

Висновки й перспективи подальших досліджень

Таким чином, ефективність виявлення ІЗ за результатами моніторингу ВДІ та оцінювання їх рівня може бути підвищено шляхом удосконалення відповідних систем на рівні організаційного, технічного та науково-методичного забезпечення.

На рівні технічного забезпечення запропоновано підхід до структурно-параметричного синтезу розрізнених АРМ, де із застосуванням евристичного методу для визначення складу, призначення та функцій системи проведено її структуризацію; використовуючи методи багатокритерійної оптимізації, визначено оптимальний склад компонентів системи та обґрунтовано їх параметри; враховуючи зміну навантаження на компоненти системи, проведено адаптивний перерозподіл наявних засобів моніторингу. У результаті на етапі впровадження системи без залучення додаткових технічних засобів підвищено ефективність охоплення ВДІ в 1,5 рази порівняно з існуючими процедурами добування й обробки даних моніторингу. Крім того, при дослідженні синтезованої системи встановлено, що на етапі її експлуатації постійна зміна навантаження на компоненти системи призводить до зниження ефективності виконання системою свого призначення через невідповідність жорсткої структури динамічному характеру вирішуваних завдань. Алгоритм адаптивного реконфігурування системи усуває виявлену суперечність і дозволяє додатково підвищити ефективність виявлення ІЗ за даними моніторингу ВДІ в період найбільш інтенсивного надходження повідомлень у 1,8 рази. На рівні технічного забезпечення запропоновано підхід до структурно-параметричного синтезу розрізнених АРМ, де із застосуванням евристичного методу для визначення складу,

Таблиця 2 – Результати застосування алгоритму адаптивного реконфігурування

Часовий інтервал	Інформаційний потік, повід.	Повнота охоплення динамічних ВДІ				Ефект, рази	
		Без реконфігурування		З реконфігуруванням			
		$B'_{сп.}$, АРМ	$F'_{сп.}$	$B''_{сп.}$, АРМ	$F''_{сп.}$		
0.00–10.00	**2540**	3	1200	2–3	897	↓0,75	E_1
10.00–20.00	**13768**	3	1200	4–6	2170	↑1,8	E_2
20.00–0.00	**3447**	3	480	3–4	583	↑1,2	E_3
За добу	**19755**	3	**2880**	2–6	**3650**	**↑1,3**	E

призначення та функцій системи проведено її структуризацію; використовуючи методи багатокритерійної оптимізації, визначено оптимальний склад компонентів системи та обґрунтовано їх параметри; враховуючи зміну навантаження на компоненти системи, проведено адаптивний перерозподіл наявних засобів моніторингу. У результаті на етапі впровадження системи без залучення додаткових технічних засобів підвищено ефективність охоплення ВДІ в 1,5 рази порівняно з існуючими процедурами добування й обробки даних. Крім того, при дослідженні синтезованої системи встановлено, що на етапі її експлуатації постійна зміна навантаження на компоненти системи призводить до зниження ефективності виконання системою свого призначення через невідповідність жорсткої структури динамічному характеру вирішуваних завдань. Алгоритм адаптивного реконфігурування системи усуває виявлену суперечність і дозволяє додатково підвищити ефективність виявлення ІЗ за даними моніторингу ВДІ в період найбільш інтенсивного надходження повідомлень у 1,8 рази.

Перспективними напрямками подальших досліджень слід вважати узагальнення запропонованого підходу до синтезу системи виявлення ІЗ за результатами моніторингу ВДІ для територіально розподілених спеціальних підрозділів.

Література

1. Артюшин Л.М. Теоретичні аспекти стратегії воєнної безпекисуспільства ідержави: [монографія]/ [Л.М. Артюшин, Г.Ф. Костенко]. – Х. : Вид-во НУВС, 2003. – 176 с. **2. Шинкарук О.М.** Основи інформаційно-аналітичної діяльності в Державній прикордонній службі України : підручник /О.М. Шинкарук, Л.М. Артюшин, В.А. Кириленко, І.І. Стоянов. – Хмельницький : Видавництво НАДПСУ, 2017. – 380 с. **3. Левченко О.В.** Проблеми і шляхи формування системи інформаційної безпеки держави / О.В. Левченко // Збірник наукових праць Харківського університету Повітряних сил. – 2014. – Вип. 2. – С. 166-168. – Режим доступу: http://nbuv.gov.ua/UJRN/ZKhUPS_2014_2_43. **4. Грищук Р.В.** Основи кібернетичної безпеки : монографія / Р.В. Грищук, Ю.Г. Даник ; за заг. ред. проф. Ю.Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.: іл. **5. Закон України** «Про Збройні Сили України» № 1934-XII від 06.12.1991 [Електронний ресурс] – Режим доступу : http://zakon0.rada.gov.ua/laws/show/1934-12/print1452609776773692. **6. Указ Президента України** №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [Електронний ресурс] – Режим доступу : http://www.president.gov.ua/documents/472017-21374. **7. Левченко О.В.** Методика виявлення заходів негативного інформаційного впливу на основі аналізу відкритих джерел / О.В. Левченко, О.М. Косогов // Системи обробки інформації. – 2016. – Вип. 1. – С. 100–102. – Режим доступу: http://nbuv.gov.ua/UJRN/soi_2016_1_22. **8. Горбулін В.П.** Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К. : Інтертехнологія, 2009. – 164 с. **9. Бурячок В.Л.** Основи формування державної системи кібернетичної безпеки : монографія / В.Л. Бурячок. – К. : НАУ, 2013. – 432 с. **10. Корченко О.** Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О. Корченко, В. Бурячок, С. Гнатюк // Безпека інформації. – 2013. – Т. 19, № 1. – С. 40–44. – Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2013_19_1_9. **11. Хорошко В.О.** До питання організації та проведення моніторингу у кібернетичному просторі / В.О. Хорошко, В.Л. Бурячок, Г.М. Гулак // Наука і оборона. – 2011. – № 2 – С. 19–23. **12. Ventre D.** Cyberwar and information warfare / Daniel Ventre. – Wiley-ISTE, 2011. – 448 p. **13. Ланде Д.В.** Програмно-апаратний комплекс інформаційної підтримки прийняття рішень : науково-методичний посібник / Д.В. Ланде, В.М. Фурашев, О.М. Григор'єв. – К. : Інжиніринг, 2006. – 48 с. **14. Казенников А.О.** Разработка моделей и алгоритмов для комплекса автоматической обработки и анализа потоков новостных сообщений на основе методов компьютерной лингвистики : дис. … канд. техн. наук : 05.13.15 – М., 2014. – 155 с. – Библиогр.: с. 113–128. **15. Писарчук А.А.** Модели ситуационного управления и самоорганизации в задачах структурно-параметрического синтеза и идентификации для сложных распределенных информационно-управляющих систем / А.А. Писарчук // Вісник Інженерної академії України. – 2014. – Вип. 2. – С. 272-275. – Режим доступу: http://nbuv.gov.ua/UJRN/Viau_2014_2_59.

ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ВЫЯВЛЕНИЯ И ОЦЕНИВАЯ ИНФОРМАЦИОННЫХ УГРОЗ

***Леонид Михайлович Артюшин** (д-р техн. наук, профессор)[1]*
***Сергей Викторович Чернышук** (канд. техн. наук)[2]*

[1]Государственный научно-исследовательский институт авиации, Киев, Украина
[2]Житомирський военный институт имени С. П. Королёва, Житомир, Украина

В статье рассмотрен типовой порядок организации и ведения мониторинга открытых источников информации специальными подразделениями Вооруженных Сил Украины в интересах

выявления и оценивания уровня информационных угроз. Проанализированы существующие подходы к выявлению и оцениванию информационных угроз, установлены их преимущества и недостатки, определены показатели, временные и ресурсные ограничения данного вида деятельности в Вооруженных Силах Украины. Сформулирована и формализована задача повышения эффективности выявления и оценивания уровня информационных угроз. Определены особенности мониторинга открытых источников информации с точки зрения его организационного, технического и научно-методическом обеспечения.

На уровне функционирования средств мониторинга открытых источников информации предложено пути повышения эффективности системы выявления и оценивания уровня информационных угроз. В частности, разработано механизм рационального использования ограниченного количества таких средств, который предусматривает согласование их работы путем объединения в единую целостную систему, способную к адаптивному переконфигурированию для наилучшего приспособления к изменению условий применения. Для этого решена задача синтеза системы выявления информационных угроз по результатам мониторинга открытых источников информации. Решение данной задачи реализовано в три этапа: определены назначение, функции и состав системы; определен количественный и качественный состав компонентов системы и обоснованы их параметры; выполнено адаптивное перераспределение имеющихся технических средств с учетом изменения нагрузки на компоненты системы.

Ключевые слова: *информационные угрозы, открытые источники информации, повышение эффективности, Вооруженные Силы Украины*.

APPROACHES OF IMPROVEMENT OF EFFECTIVENESS OF INFORMATION THREATS DETECTION AND ESTIMATION SYSTEM

Leonid M. Artushin *(Doctor of Technical Science, Professor)*[1]
Serhii V. Chernyshuk (*Candidate of Technical Sciences*)[2]

[1] ***State research institute of aviation, Kyiv, Ukraine***
[2] ***Zhytomyr military institute named after S. P. Korolov, Zhytomyr, Ukraine***

Typical organization and establishment procedures of open source monitoring by special units of Ukrainian Armed Forces for information threats detection and evaluation purposes are considered in this article. Analysis of existing approaches for information threats detection and evaluation is conducted. Their advantages and disadvantages are defined. Parameters, time and resources limitations for this activity is investigated. Main specifics and peculiarities of open source intelligence from the point of view organizational, technical and methodological support are defined.

Employed approaches to information threats detection and evaluation are analyzed, their advantages and disadvantages are revealed. On the basis of attained results necessity of improvement of effectiveness of cyber threats detection and estimation by special units of Armed Forces of Ukraine showed and directions of further development of processes at issue are defined. Measurements and criteria of effectiveness are substantiated. Formalized statement of problem of improvement of effectiveness of cyber threats detection and estimation in Armed Forces of Ukraine on basis of open source monitoring results is presented. Approaches of mentioned problem solving proposed.

Keywords: *information threats, open source intelligence, improvement of effectiveness, Armed Forces of Ukraine.*

References

1. Artyushin L.M., Kostenko H.F. (2003), Theoretic aspects of military security strategy of society and state [Teoretychni aspekty stratehii voiennoi bezpeky suspilstva i derzhavy : monohrafiia] – Kh. : Vyd-vo NUVS, 2003. – 176 p. **2. Shinkaruk O.M.,** Artyushin L.M., Kirilenko V.A., Stoyanov I.I. (2017), Basics of information-analitical actitvity in State border guard service of Ukraine: quide-book. [Osnovi informatsiyno-analitichnoyi diyalnosti v derzhavniy prikordonniy sluzhbi Ukrayini : pidruchnik], Hmelnitskiy, Vidavnitstvo NADPSU, – 380 p. **3. Levchenko O.V.** (2014), Problems and ways of state informational security system formation. [*Problemi I shlyahi formuvannya sistemi informatsiynoyi bezpeki derzhavi*], Zbirnik naukovih prats Harkivskogo universitetu Povitryanih sil. – available at: http://nbuv.gov.ua/UJRN/ZKhUPS_2014_2_43. **4. Grischuk R.V.** (2016), Cybersecurity basics : monograph [Osnovi kibernetichnoyi bezpeki : monografIya], Zhitomir: ZhNAEU, 636 p. **5. Act of Ukraine** «On Armed Forces of Ukraine» № 1934-XII from 06.12.1991 [Zakon Ukrayini «Pro zbroyni sili Ukrayini»] – available at: http://zakon0.rada.gov.ua/laws/show/1934-12/print1452609776773692. **6. Ukrainian President Decree** No.47/2017 «On decision of National Security and Defense Council of Ukraine from 29 December 2016

«On Information security policy of Ukraine» [Ukaz prezidenta Ukrayini No.47/2017 «Pro rishennya Radi natsionalnoyi bezpeki i oboroni Ukrayini vid 29 grudnya 2016 roku «Pro Doktrinu informatsiynoyi bezpeki Ukrayini»] – available at: http://www.president.gov.ua/documents/472017-21374.

7. Levchenko O.V., Kosogov O.M. (2016), Methodics of negative information influence actions detection based on open source analysis. [Metodika viyavlennya zahodIv negativnogo informatsiynogo vplivu na osnovi analizu vidkritih dzherel], Sistemi obrobki informatsiyi, No. 1, pp. 100-102 – available at: http://nbuv.gov.ua/UJRN/soi_2016_1_22. **8. Gorbulin V.P.** (2009), Information operations and society security: threats, counteraction, simulation: monograph. **[**Informatsiyni operatsiyi ta bezpeka suspilstva: zagrozi, protidiya, modelyuvannya: monografiya], Kyiv, Intertehnologiya – 164 p. **9. Buryachok V.L.** (2013), Basics of state cybersecurity system development: monograph [Osnovi formuvannya derzhavnoyi sistemi kibernetichnoyi bezpeki : monografiya], Kyiv, NAU – 432 p. **10. Korchenko O.,** Buryachok V., Gnatyuk S. (2013), State cybersecurity: attributes and problematic aspects. [Kibernetichna bezpeka derzhavi: harakterni oznaki ta problemni aspekti], Bezpeka informatsiyi, No.1, pp. 40–44. **11. Horoshko V.O**., Buryachok V.L., Gulak G.M. (2011), On the question of organization and execution of monitoring in cyberspace. [Do pitannya organizatsiyi ta provedennya monitoringu u kibernetichnomu prostori], Nauka i oborona, No.2, 19–23 p. **12. Ventre D.** Cyberwar and information warfare / Daniel Ventre. – Wiley-ISTE, 2011. – 448 p. **13. Lande D.V.,** Furashev V.M., Grigorev O.M. (2006), Program-algorithmic complex of informational decision support: instructional guide. [Programno-aparatniy kompleks informatsiynoyi pidtrimki priynyattya rishen: naukovo-metodichniy posibnik], Kyiv, Inzhiniring, p. 48. **14. Kazennikov A.O.** (2014), Models and algorithms development for complex of automatically processing and news messages stream analysis based on computer linguistic methods: dissertation in support of candidature for a technical degree. [Razrabotka modeley i algoritmov dlya kompleksa avtomaticheskoy obrabotki i analiza potokov novostnyih soobscheniy na osnove metodov kompyuternoy lingvistiki: dis. … kand. tehn. nauk], Moskov, 155 p. **15. Pisarchuk A.A.** (2014), Models of situational management and selforganisation in structural-parametric synthesis and identification in complex distributed information-management sistems [Modeli situatsionnogo upravleniya i samoorganizatsii v zadachah strukturno-parametricheskogo sinteza i identifikatsii dlya slozhnyih raspredelennyih informatsionno-upravlyayuschih system], VIsnik inzhenernoyi akademiyi Ukrayini No.2, pp.272-275 – available at: http://nbuv.gov.ua/UJRN/ Viau_2014_2_5.