DOI:**10.33099/2311-7249/2022-45-3-27-31**

УДК 004.94:355

Валерій Олександрович Крайнов *(кандидат технічних наук, доцент)*
Роман Іванович Грозовський *(кандидат військових наук)*
Ірина Вікторівна Новікова

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ОБҐРУНТУВАННЯ ВИМОГ ДО КОМПЛЕКСНОЇ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ УПРАВЛІННЯ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Питання створення комплексної системи інформаційної безпеки органів управління військового призначення – важлива частина концепції впровадження нових інформаційних технологій в військову справу. В умовах збройної агресії російської федерації значно виросли загрози інформаційній безпеці держави. Ключове завдання системи інформаційної безпеки забезпечити створення передумов для розвитку такого потенціалу інформаційної сфери України, за якого забезпечується її випереджальний розвиток, а зовнішні негативні впливи не створюють реальних небезпек національній інформаційній безпеці держави. Тому в скрутній економічній обстановці, яка склалася на сьогоднішній день в Україні, виключно актуальною стала проблема розумного, науково обґрунтованого та ефективного використання вкрай обмежених матеріальних ресурсів та пошук нових можливостей забезпечення інформаційної безпеки органів управління військового призначення з урахуванням переходу від традиційної форми подання системи захисту інформації до широкого розуміння інформаційної безпеки держави у сфері оборони в умовах воєнного стану. Суть нового уявлення полягає у реалізації комплексного підходу до розуміння інформаційної безпеки як сукупності основних напрямків захисту інформації, захисту від інформації та формування безпекового середовища в умовах воєнного стану. Це стосується і робіт по створенню, впровадженню та експлуатації комплексної системи інформаційної безпеки органів управління військового призначення. Особливого значення набуває необхідність обґрунтування вимог до комплексної системи інформаційної безпеки органів управління військового призначення як на етапе проектування так і при створенні, впровадженні та експлуатації.

Ключові слова: *комплексна система інформаційної безпеки, орган управління військового призначення, національна інформаційна безпека держави, складові системи інформаційної безпеки, цілісність інформації, конфіденційність і захищеність від несанкціонованого доступу.*

Вступ

Одним з найбільш пріоритетних напрямків розвитку Збройних Сил України є створення, розвиток і удосконалення автоматизованих інформаційних систем військового призначення. Це обумовлюється важливістю завдань саме керівництва, зростанням складності і обсягу завдань управління, вимогами до якісних параметрів їх вирішення у стислі терміни, а також інтенсивним розвитком та впровадженням для потреб ЗС України технічних систем автоматизації, у тому числі обчислювальних засобів, математичного, програмного і інформаційного забезпечення. Життєдіяльність ЗС України цілком визначається рівнем розвитку, якістю функціонування і безпекою інформаційного середовища. Інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. Процес прийняття рішення в органах управління військового призначення (ОУВП) значно залежить від інтенсивності інформаційного обміну, повноти, своєчасності, достовірності інформації. В умовах загрози кібербезпеки інформаційній структурі держави [5] особливого значення набуває пошук нових можливостей забезпечення інформаційної безпеки з урахуванням формування нового поля протиборства – кіберпростору, коли інформація в електронному форматі стає дуже дорогим товаром, і проблема захисту інформації виходить на перший план. Проблем інформаційної безпеки безліч, тому в першу чергу необхідно вирішувати питання, по'вязані з визначенням природи різних видів інформаційних небезпек (загроз), механізмів їхнього впливу на об'єкти інформаційної безпеки, можливих наслідків цих впливів, шляхів і методів їх нейтралізації або зменшення. Комплексність системи інформаційної безпеки (СІБ) досягається охопленням всіх можливих загроз і узгодженням між собою різних методів і засобів, що забезпечують захист всі елементів органів управління військового призначення [1].

Постановка проблеми. При створенні комплексної системи інформаційної безпеки (КСІБ) необхідно захищати інформацію у всіх фазах її існування – як електронної (що міститься

© В.О.Крайнов, Р.І.Грозовський, І.В.Новікова

та обробляється в автоматизованих інформаційних системах або на машинних носіях), так і документальної (паперові документи). У комплексній системі інформаційної безпеки органів управління військового призначення (КСІБ ОУВП) захищати інформацію необхідно не лише від несанкціонованого доступу до неї, а й від несанкціонованого втручання в процес її обробки, зберігання та передачі, спроб порушення працездатності програмно-технічних засобів тощо.

При побудові КСІБ ОУВП виділяють дві групи вимог до захищеності органів управління військового призначення [1,2], які повинні враховуватися – формалізовані вимоги і вимоги, які сформулюються на підставі існуючої статистики загроз. Загрози СІБ ОУВП істотно залежать від функціонального призначення, умов експлуатації, від того, яка інформація зберігається і обробляється в системі, наявність в СІБ уразливих місць, апаратно-програмних особливостей автоматизованих інформаційних систем (АІС), наявності засобів захисту та їх характеристик. У силу особливостей сучасних АІС існує значне число різних видів загроз безпеці суб'єктів інформаційних відносин. Загрози мають різний характер і викликають неоднакові по значущості і об'єму наслідки. Комплексність СІБ досягається охопленням всіх можливих загроз і узгодженням між собою різнорідних методів і засобів, що забезпечують захист всіх елементів автоматизованої інформаційної системи ОУВП [4].

Аналіз остатніх досліджень і публікацій. Проблематиці інформаційної безпеці приділяють увагу багато вчених як в Україні, так і за кордоном. Особливо гостро на сьогодні, з урахуванням умов постійної конкуренції не лише між недержавними структурами, а і структурами, які містять державні інформаційні ресурси, точиться боротьба за інформацію. Тому її ключове завдання СІБ – захист усієї інформаційної інфраструктури органів управління військового призначення від будь-яких несанкціонованих дій [2]. На цю годину склалася цілком певна послідовність розробки комплексних систем забезпечення інформаційної безпеки, яка включає кілька етапів:

проектування, впровадження та супровід СІБ, що забезпечують безпеку функціонування інформаційних ресурсів органів управління військового призначення;

комплексне діагностичне обстеження, оцінка та аудит систем інформаційної безпеки, у тому числі, на відповідність існуючим стандартам.

Принципи побудови КСІБ, загальні принципи інформаційної безпеки в АІС розглядали такі фахівці у сфері захисту інформації, як В. М. Богуш, М. В. Грайворонський, О. А. Довидьков, В.В. Домарев, В. Г. Кривуца, В. Ф. Шаньгин, О. Г. Корченко, Г. Ф. Конахович, В. Г. Грибунін та інші вчені.

Таким чином, метою статті є удосконалення науково-методичного аппарату для визначення ступеня небезпеки загроз і обґрунтування вимог до КСІБ ОУВП, які дозволяли б вирішувати задачі створення, використання і оцінки ефективності СІБ для АІС, які проектуються, та існуючих інформаційних систем ОУВП [1, 4].

Виклад основного матеріалу дослідження

Система інформаційної безпеки ОУВП – це спеціалізована система, що має на меті зменшення або ліквідувати чинники загроз, умов, які сприяють прояву кожного з них і зниженню вірогідності виникнення ситуації загрози об'єкту безпеки. Тому функціонування моделі СІБ ОУВП можна представити структурною схемою (рис. 1).

Рис. 1. Структурна схема функціонування моделі СІБ ОУВП

Для обґрунтування вимог до КСІБ ОУВП необхідно розробити модель представлення системи (процесів) інформаційної безпеки, яка на основі науково-методичного апарату, дозволяла б вирішувати задачі створення, використання і оцінки ефективності СІБ для автоматизованої інформаційної системи ОУВП, які проектуються та існуючих [1]. У спрощеному вигляді структурна схема моделі СІБ для АІС представлена на рис. 2.

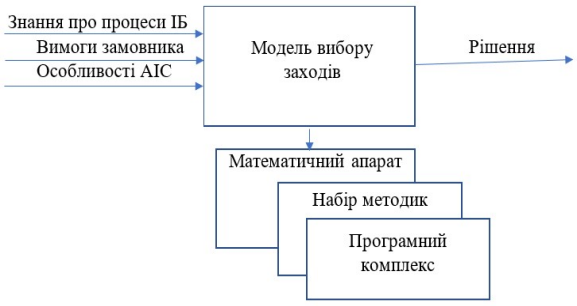

Рис. 2. Загальна модель системи інформаційної безпеки автоматизованої інформаційної системи ОУВП

Основним завданням моделі є наукове забезпечення процесу створення інформаційної безпеки за рахунок правильної оцінки ефективності прийнятих рішень і вибору раціонального варіанту організаційно-технічної реалізації системи захисту інформації. Специфічними особливостями рішення задачі створення КСЗІБ є: неповнота і невизначеність вихідної інформації про склад АІС і характерних загрозах; багатокритеріальність задачі, пов'язана з необхідністю урахування великої кількості часткових показників (вимог) до системи інформаційної безпеки ОУВП; наявність як кількісних, так і якісних показників, які необхідно враховувати при рішенні задач розробки

і впровадження системи інформаційної безпеки ОУВП; неможливість застосування класичних методів оптимізації.

Така модель СІБ повинна задовольняти наступним вимогам:

1. Використовуватися в якості: методики формування показників і вимог до КСЗІБ; інструменту (методики) оцінки ефективності комплексної системи інформаційної безпеки ОУВП; моделі КСЗІБ для проведення досліджень (матриця стану).

2. Володіти властивостями: універсальності; комплексності; простоти використання; наочності; практичної спрямованості; функціонувати в умовах високої невизначеності вихідної інформації.

3. Дозволяти: встановлювати взаємозв'язок між показниками (вимогами); задавати різні рівні захисту; отримувати кількісні оцінки; контролювати стан СІБ; застосовувати різні методики оцінок; оперативно реагувати на зміни умов функціонування.

Методика вибору раціонального варіанту рішення щодо проведення заходів інформаційної безпеки залежить від повноті вихідних даних та часу, виділеного на прийняття рішення. Проведений аналіз методів визначення ступеня небезпеки загроз і важливості часткових показників якості СІБ показав, що запропонований підхід, на відміну від існуючих, дозволяє врахувати фізичну сутність показників і відносини між ними, складність проведення експертизи і трудомісткість одержання експертної інформації, ступінь погодженості думок експертів, трудомісткість обробки експертних даних [1-3]. З урахуванням зазначених факторів обрано метод Сааті Т.Л. [6], що базується на формуванні матриці парних порівнянь важливості показників. Відповідно до цього методу необхідно вирішити матричне рівняння

$$(A-\lambda E)W=0, \quad (1)$$

де А –матриця парних порівнянь;

Е – одинична матриця;

W – власний вектор;

λ– власне значення матриці.

Координати власного вектору W і визначають важливість показників. Проведений аналіз методів побудови функцій належності показників організації та відповідність проведених заходів інформаційної безпеки необхідному рівню якості показав, що найбільш простим у реалізації є метод, що базується на ідеї розподілу ступеня належності елементів множин з визначеною ознакою відповідно до їхніх рангів, отриманих експертним методом [2].

Під рангом елемента $x_i \in X$ розуміється число $r_s(x_i)$, що характеризує значимість цього елемента у формуванні властивості, що описується нечітким термом S. Допускаємо, що виконується правило: чим більший ранг елемента, тим більше ступінь належності. Тоді розподіл ступенів належності задається у вигляді співвідношення:

$$\frac{\mu_1}{r_1} = \frac{\mu_2}{r_2} = \ldots = \frac{\mu_n}{r_n} \quad (2)$$

до якого додається умова нормування

$$\mu_1 + \mu_2 + \ldots + \mu_n = 1 \quad (3)$$

де $r_i = r_s(x_i)$; $\mu_i = \mu_s(x_i)$; $i = 1, n$.

Це дозволить отримати систему рівнянь та знаходити значення ступенів належності :

$$\left.\begin{array}{l} \left(1+\frac{r_2}{r_1}+\frac{r_3}{r_1}+\ldots+\frac{r_n}{r_1}\right)^{-1} \\ \left(\frac{r_1}{r_2}+1+\frac{r_3}{r_2}+\ldots+\frac{r_n}{r_2}\right)^{-1} \\ \left(\frac{r_1}{r_n}+\frac{r_2}{r_n}+\frac{r_3}{r_n}+\ldots+1\right)^{-1} \end{array}\right\} = \mu_1 \quad (4)$$

Приклад побудови такої функції належності наведено на рис. 3 .

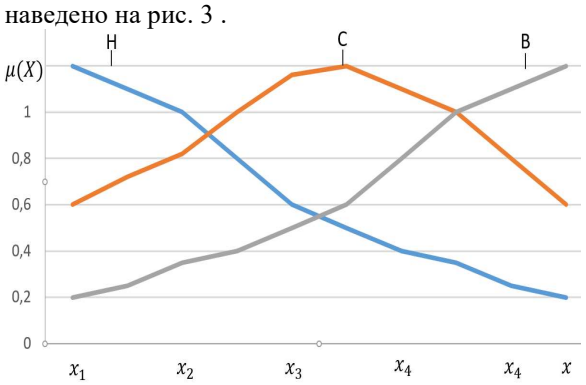

Рис. 3. Приклад побудови функції належності

Проведений аналіз методів рішення задач нечіткої багатокритеріальної оптимізації дозволяє розробити алгоритми рішень задач такого класу, виробляти рекомендації з вибору методу і раціонального варіанта рішення задач з врахуванням кількісних і якісних показників в залежності від виду експертної інформації про перевагу показників (табл. 1).

Таблиця 1

Рекомендації з вибору методу рішення задачі в залежності від видуекспертної інформації про перевагу показників

Експертна інформація про ступінь чи переваги важливості показників	Метод рішення багатокритеріальної задачі
відсутня	мінімаксний метод
показники упорядковані за важливістю	лексикографічний метод
визначено вагові коефіцієнти показників	адитивний показник мультиплікативний показник мінімаксний показник

Методика вибору раціонального варіанту рішення щодо проведення заходів інформаційної безпеки залежить від вихідних даних та часу, виділеного на прийняття рішень.

Так при рівній важливості показників вихідну інформацію доцільно представить у вигляді матриці часткових показників для кожного варіанту реалізації (табл. 2).

Нехай є m показників, то кращим вважається варіант, що забезпечує найкраще значення всіх показників. Правило вибору може бути записане у

вигляді перерахування відповідних множин:

$$D(\overline{X_i}) = q_1(\overline{X_i}) \wedge \ldots \wedge q_l(\overline{X_i}) \wedge \mu_{l+1}(\overline{X_i}) \wedge \ldots \wedge \mu_m(\overline{X_i}) \quad (5)$$

Операції перетину нечітких множин відповідає операція *min*, тобто

$$Q_D(\overline{X_i}) = \min_{\substack{j=1,m \\ i=1,n}} \{q_1(\overline{X_i}), \ldots, q_l(\overline{X_i}), \mu_{l+1}(\overline{X_i}), \ldots, \mu_m(\overline{X_i})\} \quad (6)$$

Як оптимальний обираємо варіант, у якому відповідає найбільше значення функції $Q_D(\overline{X_i})$

$$Q_D(\overline{X_{l_0}}) = \max_{i=1,n} Q_D(\overline{X_i}) \quad (7)$$

Таблиця 2

Матриця часткових показників для варіантів реалізації

Варіант $X_i; i = 1,n$ Показник $q_j; j = 1,m$	$\overline{X_1}$	$\overline{X_1}$	…	$\overline{X_1}$
$q_1(\overline{X_i})$	$q_1(\overline{X_1})$	$q_1(\overline{X_2})$	…	$q_1(\overline{X_n})$
…	…	…	…	…
$q_l(\overline{X_i})$	$q_l(\overline{X_1})$	$q_l(\overline{X_2})$	…	$q_l(\overline{X_n})$
$\mu_{l+1}(\overline{X_i})$	$\mu_{l+1}(\overline{X_1})$	$\mu_{l+1}(\overline{X_2})$		$\mu_{l+1}(\overline{X_n})$
…	…	…	…	…
$\mu_m(\overline{X_i})$	$\mu_m(\overline{X_1})$	$\mu_m(\overline{X_2})$		$\mu_m(\overline{X_n})$

У випадку, якщо показники q_j мають різну важливість, кожному з них приписується число (чим вище показник, тим більше a_j). При цьому дотримується умова: $a_j \geq 0; \sum_{j=1}^{m} a_j = 1$.

Загальне правило вибору методів визначення коефіцієнтів важливості приймає вигляд:

$$Q_D(\overline{X_i}) = q_1^{a_1}(\overline{X_i}) \wedge \ldots \wedge q_l^{a_1}(\overline{X_i}) \wedge \mu_{l+1}^{a_1}(\overline{X_i}) \wedge \ldots \wedge \mu_m^{a_m}(\overline{X_i}) \quad (8)$$

Кращий варіант l_0 знаходиться зі співвідношення:

$$Q_D(\overline{X_{l_0}}) = \max_{i=1,n} \min_{j=1,m} \{q_1^{a_1}(\overline{X_i}), \ldots, q_l^{a_1}(\overline{X_i}), \mu_{l+1}^{a_1}(\overline{X_i}), \ldots, \mu_m^{a_m}(\overline{X_i})\}$$

Лексикографічний метод вибору рішення задачі [4] щодо відшукування оптимального варіанту проведення заходів інформаційної безпеки АІС ОУВП зводиться до упорядкування показників по ступені переваги (важливості):

$$q_1 > q_2 > \cdots > q_j > \cdots > q_m; j = 1,m$$

За згодою особи, що приймає рішення (ОПР), для кожного показника призначається величина припустимої поступки $\triangle q_j; j = 1,m$, у межах якої розглянуті варіанти проведення заходів інформаційної безпеки вважаються "практично рівноцінними". Для першого показника q_1 формується множина "практично рівноцінних" варіантів (множина π_1), що задовольняють умові:

$$\max_{i=1,n} q_1(\overline{X_i}) - \underset{K=1,n}{q_1}(\overline{X_K}) \leq \Delta q_1 \quad (9)$$

Якщо π_1-множина містить рівно один варіант, то він і вважається найкращим. Якщо кілька, то розглядаються усі варіанти множини π_1 по показнику q_2.

Для другого показника q_2 формується π_2-множина варіантів з множини π_1, що задовольняють умові:

$$\max_{i \in \pi_1} q_2(\overline{X_i}) - \underset{K \in \pi_1}{q_2}(\overline{X_K}) \leq \Delta q_2 \quad (10)$$

Якщо π_2-множина містить рівно один варіант, то він і вважається найкращим: якщо більш одного – розглядаємо ці варіанти по показнику q_3 і т.д.

Якщо всі показники послідовно переглянуті і в результаті одержуємо множину $\pi = \pi_1 \pi_2 \pi_m$, що містить більше однієї альтернативи, то можливо застосувати два переходи: зменшити величину припустимої поступки Δq_j, починаючи з першого по важливості показника і повторити всі кроки рішення; надати ОПР остаточний вибір найкращого варіанта.

Висновки й перспективи подальших досліджень

Система інформаційної безпеки функціонування ОУВП потребує реформування. Проведений аналіз існуючих загроз показав доцільність створення комплексної СІБ для визначеної множини критичної інформації та нейтралізації загроз. Комплексна система інформаційної безпеки органів управління військового призначення повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в умовах ведення бойових дій.

В умовах сучасної інформаційної та кібервійни, яка ведеться проти нашої країни, забезпечення безпеки автоматизованих інформаційних систем органів військового управління має стати державним завданням. Це потребує подальшого удосконалення науково-методичного аппарату для визначення ступеня небезпеки загроз і обґрунтування вимог до КСІБ ОУВП, які дозволяли б вирішувати задачі створення, використання і оцінки ефективності СІБ для існуючих інформаційних систем ОУВП та і для тих, які проектуються.

Література

1. Крайнов В.О., Маланчук М.Ф., Грозовський Р.І. Методика оцінки ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління. К.: НУОУ, Сучасні інформаційні технології у сфері безпеки та оборони, 2020р. № 1(37),- С. 103-106. **2. Маланчук М.Ф.**, Крайнов В.О., Поліщук А.С. Методика експертизи результатів експертного оцінювання. К.: НУОУ, Сучасні інформаційні технології у сфері безпеки та оборони, 2020р. № 2(38),- С. 33-38. **3. Домарев В.В**. Безопасность информационніх технологий. Методология создания защиті. – К. ООО :"ТИД ДС", 2002. – 688 с. **4.** Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с. **5. Демченко П**. Кібернетична безпека як новітній напрям інформаційної складової національної безпеки України: конституційно-правовий аспект. Вісник Львівського національного університету імені І. Франка.2018. Вип. 67. (Серія «Юридична»). **6. Саати** Т. Л. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1989. — 316 с.

JUSTIFICATION OF REQUIREMENTS FOR THE INTEGRATED SYSTEM OF INFORMATION SECURITY OF MILITARY ADMINISTRATION BODIES

Valerii Krainov *(Candidate of technical sciences, associate professor)*
Roman Hrozovskyi *(Candidate of military sciences)*
Iryna Novikova

National Defense University of Ukraine named after Ivan Chernyakhovskyi, Kyiv, Ukraine

The issue of creating an integrated information security system for military command and control bodies is an important part of the concept of introducing new information technologies into military affairs. In the conditions of armed aggression of the Russian Federation, the dangers of the information security of the state have increased significantly. The key role of the information security system is to ensure the creation of prerequisites for the development of such a potential of the information sphere of Ukraine, which ensures its advanced development, and external negative influences do not create real dangers to the national information security of the state.

Therefore, in the difficult economic situation that has developed in Ukraine today, the problem of reasonable, scientifically based and efficient use of extremely limited material resources and the search for new opportunities for ensuring the information security of military command and control bodies, taking into account the transition from the traditional form of presenting the information security system, has become extremely relevant. to a broad understanding of the information security of the state in the field of defense under martial law.

The essence of the new idea is to implement an integrated approach to understanding information security as a combination of the main areas of information protection, protection from information and the formation of a security environment in a state of martial law. This also applies to work on the creation, implementation and operation of an integrated information security system for military command and control bodies. Of particular importance is the need to justify the requirements for an integrated information security system for military command and control bodies both at the design stage and during creation, implementation and operation.

Key words*: integrated information security system, military administration, national information security of the state, components of information security systems, information integrity, confidentiality and protection from unauthorized access.*

References

1. Krainov V.O., Malanchuk M.F., Grozovsky R.I. Methodology for evaluating the effectiveness of a complex system for the protection of information of automated information systems of the bodies of the military administration. K .: NUOU, Modern information technologies in the field of security and defense, 2020. No. 1 (37), - S. 103-106. **2. Malanchuk M.F.,** Krainov V.O., Polishchuk A.S. Methodology for the examination of the results of expert evaluation. K .: NUOU, Modern information technologies in the field of security and defense, 2020. No. 2 (38), - S. 33-38. **3. Domarev V.V.** Security of information technologies. Methodology for creating protection. - K. OOO: "TID DS", 2002. - 688 p. **4.** Protection of information in automated control systems: a guidebook / Uklad. I. A. Pilkevich, N. M. Lobanchikova, K. V. Molodetska. - Zhytomyr: Type of waiting for them. I. Franka, 2015.-226 p. **5. Demchenko P.** Cybernetic security as a novel direct information warehouse national security of Ukraine: constitutional and legal aspect. Bulletin of Lviv National University named after I. Frank. 2018. Vip. 67. (Series "Legal"). **6. Saati T. L.** Decision-making. Method of hierarchy analysis. — M.: Radio and Communications, 1989. – 316 p.