DOI: **10.33099/2311-7249/2024-51-3-120-132**

УДК: 004.056.5

Сулімовська Марія Володимирівна

Національний університет оборони України, м. Київ, Україна

УДОСКОНАЛЕНА МЕТОДИКА ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ, ЯКА ЦИРКУЛЮЄ В ПІДСИСТЕМІ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ

У статті сформульовано актуальне завдання оцінювання захищеності інформації з обмеженим доступом, яка циркулює в підсистемі органів військового управління системи управління оперативного угруповання військ (сил) під час виконання операцій у зоні проведення бойових дій та запропоновано її вирішення. Аналіз функціонування оперативного угруповання військ (сил) підтверджує, що ця проблема є актуальною і потребує вирішення в умовах широкомасштабної збройної агресії російської федерації проти України. Метою статті є вдосконалення методики оцінювання захищеності інформації з обмеженим доступом, яка циркулює в підсистемі органів військового управління, що здійснене для запобігання витоку інформації та недопущення втрати її матеріальних носіїв й унеможливлення використання цих відомостей противником. Методи дослідження: системний аналіз, метод моделювання, експертні оцінки, метод порівняльного аналізу, метод SWOT-аналізу, метод статистичного аналізу, метод сценарного аналізу. Зазначений методологічний підхід дав змогу належно оцінити захищеність інформації з обмеженим доступом. Аналіз останніх досліджень і публікацій, присвячених оцінюванню захищеності інформації свідчить про необхідність актуалізації та вдосконалення такого оцінювання з урахуванням загроз захищеності, зумовлених високою динамікою бойових дій. У статті показано, що вирішення цієї проблеми потребує системного підходу та ефективного застосування показників оцінювання захищеності інформації з обмеженим доступом в підсистемі органів військового управління. Запропоновано визначення коефіцієнту захищеності інформації з обмеженим доступом, який характеризує ступінь ефективності функціонування системи забезпечення захисту інформації в підсистемі органів військового управління під час виконання операцій. Цей показник обмежується статтями Зводу відомостей, що становить державну таємницю та пунктами Переліку службової інформації, що належать до структур сектору оборони України (Збройних Сил України та Міністерства оборони України). Удосконалена методика оцінювання захищеності інформації з обмеженим доступом складається з восьми блоків, що охоплюють формування вихідних даних, розрахунок коефіцієнтів захищеності та оцінку потенційної шкоди від витоку інформації або втрати відомостей. Методика також передбачає виявлення причин невідповідності вимогам, розробку рекомендацій для підвищення ефективності забезпечення захисту та визначення загального рівня безпеки інформації. Її реалізація дає змогу забезпечити відповідність системи забезпечення захисту інформації з обмеженим доступом в підсистемі органів військового управління встановленим вимогам та мінімізувати ризики втрати матеріальних носіїв інформації. Науковою новизною є впровадження чотирьохступеневої системи обмеження доступу до інформації з грифами секретності «Особливо важливо», «Цілком таємно», «Таємно» та грифом обмеження доступу «Для службового користування». Ця система передбачена в проєкті Закону України «Про безпеку класифікованої інформації» з урахуванням положень Стратегії національної безпеки України, стандартів безпеки НАТО та Європейського Союзу. Її впровадження дає змогу створити нову методику оцінювання захищеності інформації з обмеженим доступом та вдосконалити нормативно-правову базу. Удосконалена методика сприяє розвитку теорії безпеки інформації, впроваджуючи міжнародні стандарти НАТО та Європейського Союзу в контексті національної оборони України. Це дає змогу створити уніфіковану систему оцінювання захищеності інформації та адаптувати підходи до оцінювання захищеності інформації з урахуванням сучасних загроз і специфіки оперативного середовища. Практична значущість методики надає можливість своєчасно оцінювати рівень захищеності інформації, виявляти причини виникнення загроз і розробляти заходи для мінімізації ризиків витоку або втрати відомостей. Її впровадження підвищує ефективність управління оперативним угрупованням військ (сил) в зоні проведення бойових дій. Напрямом подальших досліджень є удосконалення моделі оцінювання шкоди оперативному угрупованню військ (сил) у разі витоку інформації з обмеженим доступом, яка циркулює в підсистемі органів військового управління, а також розробка та впровадження відповідних положень у нормативно-правові акти, що регламентують організацію та забезпечення безпеки інформації.

***Ключові слова**: інформація, що становить держану таємницю, службова інформація, безпека інформації, оперативне угруповання військ (сил), коефіцієнт важливості, перелік загроз, захищеність, система забезпечення захисту інформації.*

© М.В. Сулімовська

Вступ

Постановка проблеми. Збройна агресія російської федерації проти України поставила нові виклики щодо збереження надійного функціонування системи забезпечення захисту інформації з обмеженим доступом (далі – ІзОД) в підсистемі органів військового управління (далі – ОВУ) системи управління оперативного угруповання військ (сил) (далі – ОУВ(с)). Тому, удосконалення методики оцінювання захищеності інформації з обмеженим доступом, яка циркулює в підсистемі ОВУ, з урахуванням її теоретичної та практичної значущості для сектору оборони України є науковим завданням сучасності.

Методика інтегрує міжнародні стандарти НАТО та Європейського Союзу (далі – ЄС) [6; 7] і сприяє реалізації завдання Стратегії національної безпеки України [5]. Її впровадження дасть змогу забезпечити формування єдиної системи забезпечення захисту ІзОД, враховуючи сучасні підходи до оцінювання, існуючих загроз та специфіки оперативного середовища. Практичною значущістю удосконаленої методики є можливість своєчасного оцінювання рівня захищеності ІзОД, виявлення причин загроз та розробки переліків завдань і заходів для їх усунення. Її впровадження сприяє мінімізації ризиків витоку ІзОД або втрати матеріальних носіїв інформації (далі – МНІ), а також підвищує ефективність управління оперативним угрупованням військ (сил) в зоні проведення бойових дій.

Застосування системного підходу до вирішення проблеми захищеності ІзОД дає змогу суттєво підвищити рівень безпеки інформації в підсистемі ОВУ системи ОУВ(с) та мінімізувати ризики витоку інформації. Для цього пропонується впровадження системи формальних коефіцієнтів захищеності, реалізованих через систему забезпечення захисту інформації з обмеженим доступом (далі – СЗЗІзОД). Найбільш ефективною формою цих коефіцієнтів є кількісна, яка спрощує аналіз, порівняння варіантів захищеності та оптимізацію вибору найкращих рішень. Комплексний підхід до створення СЗЗІзОД, яка циркулює в підсистемі ОВУ, забезпечує ефективну захищеність відомостей та мінімізацію потенційних загроз.

Аналіз і реагування на динамічні зміни оперативної обстановки, включно з оцінкою ризиків і ухваленням рішень в умовах обмеженого часу, є ключовими для забезпечення належного рівня захищеності ІзОД в підсистемі ОВУ системи управління ОУВ(с), які здійснюють планування, координацію дій військ та підтримують оперативну взаємодію між підрозділами для успішного виконання бойових завдань.

Аналіз останніх досліджень і публікацій. Розв'язання задач оцінювання захищеності ІзОД в підсистемі ОВУ стикається з множиною різнорідних факторів, які ускладнюють отримання точної та повної оцінки стану СЗЗІзОД. Головними чинниками, що впливають на цей процес є невизначеність і змінюваність загроз в умовах бойових дій. Розгляду зазначеної проблематики присвячена низка публікацій та джерел.

Підходи до розроблення (удосконалення) методик у сфері інформаційної безпеки базуються на положеннях Закону України «Про державну таємницю» [1], Зводу відомостей, що становить державну таємницю (далі – ЗВДТ) [3], Переліку відомостей Міністерства оборони України, які містять службову інформацію (далі – ПСІ) [4] та інших чинних нормативних документів. Так, в статті [11] аналізуються законодавчі, нормативно-правові аспекти проблем у сфері охорони державної таємниці в умовах війни та шляхи їх вирішення. Наведено матеріали щодо функціонування режимно-секретних органів в умовах війни та проведено оцінювання ефективності функціонування системи захисту інформації за окремими показниками. Але в роботі не розглянуто питання використання наведеного методу оцінювання захищеності ІзОД.

У [12] викладено науково-методичні підходи щодо оцінювання спроможностей у сфері забезпечення захисту інформації. Проведено вибір та обґрунтування показників оцінювання ефективності функціонування режимно-секретних органів, але не викладено методичний підхід щодо оцінювання ефективності функціонування системи забезпечення захисту інформації на їх основі.

У дослідженні [10] проаналізовано математичні моделі та методи вирішення проблем безпеки інформації для побудови систем забезпечення захисту інформації в автоматизованих системах суб'єктів охоронної діяльності. Наведені методи можуть бути використані для формалізованого опису процесів оцінювання захищеності ІзОД в підсистемі ОВУ.

У роботі [9] оцінювання ефективності роботи режимно-секретних органів в умовах війни (особливого періоду) здійснюється за окремими показниками без врахування важливих для підсистеми органів військового управління складових, зокрема, оперативності виконання бойових завдань.

В монографії [13] розглянуті нормативно-правові та соціально-організаційні аспекти охорони державної таємниці, проведено критичний аналіз чинних методичних настанов, рекомендацій та процедур оцінювання можливої шкоди у разі розголошення державної таємниці або втрати матеріальних носіїв секретної інформації, запропоновано оригінальні експертно-аналітичні підходи до визначення цінності секретної інформації та обсягів втрат у разі її витоку. Однак виникає потреба дослідити та вдосконалити наведену методику оцінки стану охорони державної таємниці, що на відміну від існуючої, враховує специфіку ІзОД, яка циркулює в підсистемі ОВУ системи управління ОУВ(с).

Аналіз положення стандартів безпеки НАТО та ЄС («Політика безпеки НАТО», С-М (2002) 49, «Правила безпеки ЄС», 2013/488/EU) [6; 7], які відповідно до пункту 4.12 Стратегії національної безпеки України (затверджено Указом Президента України від 26.05.2015 № 287/2015) [5] імплементовані в проєкт Закону України «Про

безпеку класифікованої інформації» [8], засвідчив необхідність переходу на чотирьохступеневу систему обмеження доступу до вказаної інформації гриф секретності «Особливо важливо», «Цілком таємно», «Таємно» та грифу обмеження доступу «Для службового користування»), удосконалення процедур віднесення відомостей до секретної інформації, засекречування та розсекречування матеріальних носіїв секретної інформації. Це дає змогу розробити нові кількісні показники оцінювання захищеності ІзОД, що інтегровані в удосконалену методику оцінювання для забезпечення її ефективного функціонування.

Проведений аналіз досліджень і публікацій стосовно оцінювання захищеності ІзОД, яка циркулює в ОВУ, свідчить про необхідність вдосконалення існуючих методик для запобігання витоку інформації або втрати відомостей, що можуть вплинути на функціонування оперативного угруповання військ (сил) і загальну ефективність виконання бойових завдань. Через це, вирішення проблеми оцінювання захищеності інформації з обмеженим доступом в підсистемі органів військового управління є актуальним науковим завданням.

Метою статті є вдосконалення методики оцінювання захищеності інформації з обмеженим доступом, яка циркулює в підсистемі органів військового управління, що здійснене для запобігання витоку інформації та недопущення втрати її матеріальних носіїв й унеможливлення використання цих відомостей противником.

Виклад основного матеріалу дослідження

Удосконалена методика призначена для оцінювання захищеності інформації з обмеженим доступом, яка циркулює в підсистемі органів військового управління та здійснюється на основі методики оцінки стану охорони державної таємниці [13] завдяки переходу на чотирьохступеневу систему обмеження доступу, що інтегруються з міжнародними стандартами НАТО та ЄС [6; 7] у секторі оборони України. Такий підхід дає змогу створити уніфіковану систему забезпечення захисту ІзОД в підсистемі ОВУ системи управління ОУВ(с).

Об’єктом дослідження удосконаленої методики є процес оцінювання захищеності ІзОД, яка циркулює в підсистемі ОВУ системи управління ОУВ(с), з урахуванням сучасних загроз і специфіки оперативного середовища. Сутність удосконаленої методики оцінювання захищеності ІзОД зводиться до розробки системи комплексного оцінювання рівня захищеності відомостей, що циркулюють у підсистемі ОВУ, і містить використання формальних коефіцієнтів захищеності. Це характеризує ступінь зниження можливих втрат, які обумовлені витоком ІзОД та втратам МНІ, а також сукупну потенційну шкоду для ОУВ(с).

Передбачено застосування системного підходу до визначення загроз захищеності відомостей і розробки ефективних заходів для їх усунення, зокрема, через врахування міжнародних стандартів безпеки та специфіки системи управління ОУВ(с). Удосконалена методика дає змогу своєчасно реагувати на зміни оперативної обстановки та забезпечувати належний захисту ІзОД в підсистемі ОВУ системи управління ОУВ(с). Ця система виконує планування та координацію дій військ, а також підтримує оперативну взаємодію між підрозділами для успішного виконання бойових завдань.

Сфера застосування удосконаленої методики обмежується її використанням в підсистемі ОВУ системи управління ОУВ(с), що здійснюють діяльність стосовно планування, координації дій військ, оцінювання оперативної обстановки, організації взаємодії між підрозділами та забезпечення безпеки ІзОД в умовах інтенсивного ведення бойових дій. Удосконалена методика спрямована на забезпечення належного рівня захисту інформації, що становить державну таємницю та службову інформації, а також на запобігання витоку інформації або втраті МНІ, що може негативно вплинути на ефективність виконання бойових завдань та функціонування оперативного угруповання військ.

Основним припущенням є те, що: $K_з^{ОВУ}$ – коефіцієнт захищеності ІзОД, характеризує ступінь ефективності функціонування системи забезпечення захисту ІзОД в підсистемі ОВУ під час виконання операцій в зоні виконання бойових дій; Кзі,j – коефіцієнт захищеності ІзОД відповідно до статей ЗВДТ (і) та пунктів ПСІ (j), що належать до структури сектору оборони України (Збройних Сил України та Міністерства оборони України). Коефіцієнт характеризує ступінь зниження можливих втрат, які обумовлені витоком ІзОД та втратам МНІ. Ввідними даними слід вважати формалізовані дані отримані на основі аналізу чинних нормативних документів у сфері захисту інформації [1; 2; 3; 4; 5; 8]. Математичний апарат, що використовується в удосконаленій методиці розроблений у [13], але потребує уточнення відповідно до наведених обмежень та припущень (рис. 1). Оцінювання захищеності ІзОД проводиться на підставі аналізу функціонування системи забезпечення захисту інформації в підсистемі ОВУ системи управління ОУВ(с) під час виконання операцій в зоні проведення бойових дій. Структурна схема удосконаленої методики наведена на рис. 1 та складається з таких блоків:

1 Блок. Формування вихідних даних. Проводиться з урахуванням розподілу ІзОД на інформацію, яка становить державну таємницю (далі – ДТ) та службову інформацію (далі – СлІ) і циркулює в підсистемі ОВУ системи управління ОУВ(с).

Для визначення $K_{з\,i,j}$ – коефіцієнту захищеності інформації з обмеженим доступом відповідно до статей ЗВДТ (*і*) та пунктів ПСІ (*j*), що належать до структури сектору оборони України. Коефіцієнт характеризує ступінь зниження можливих втрат, що обумовлені витоком ІзОД та втратами МНІ.

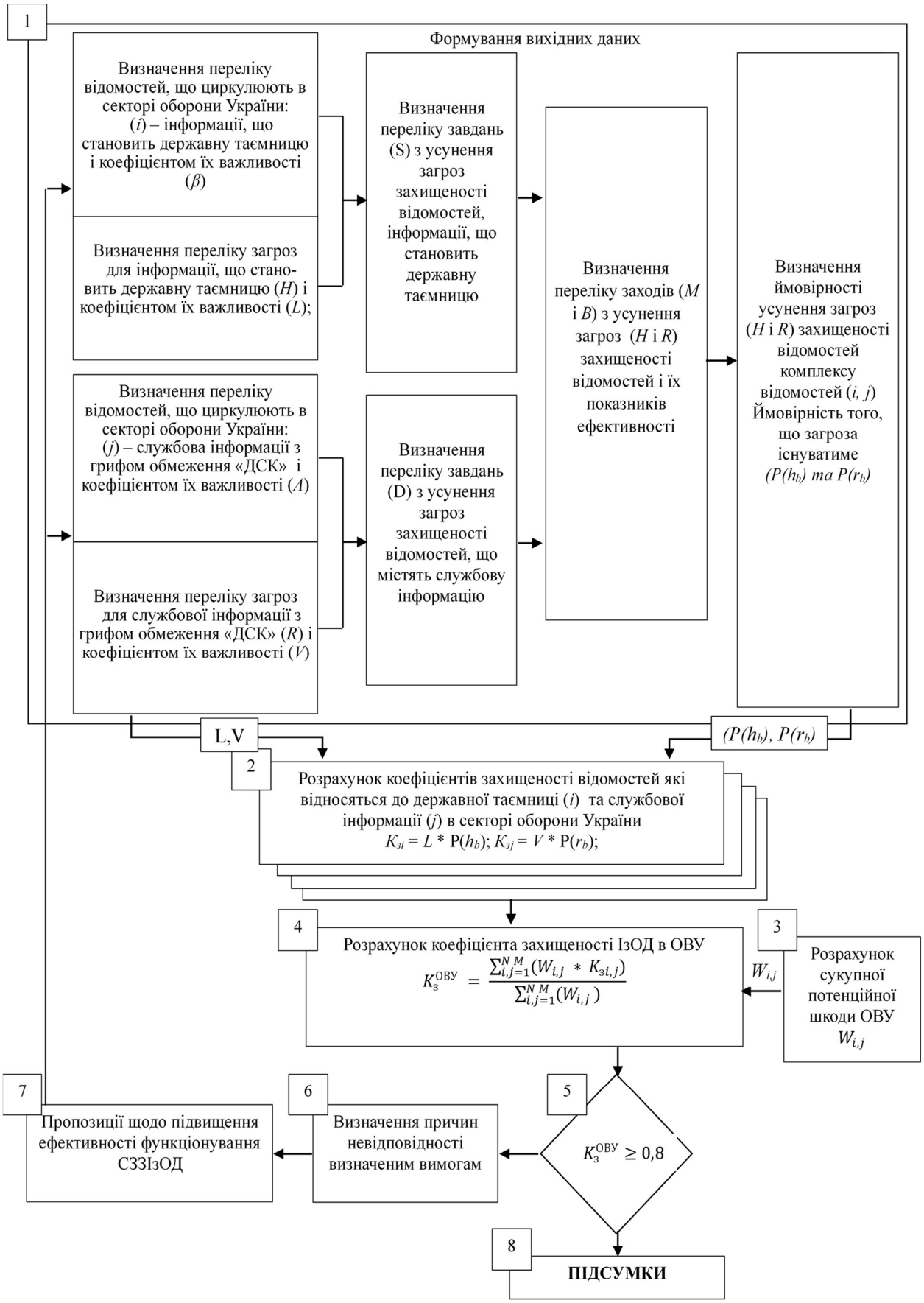

Рисунок – 1 Структурна схема удосконаленої методики оцінювання захищеності інформації з обмеженим доступом у підсистемі органів військового управління

Розглянемо етап формування вихідних даних для інформації, яка становить ДТ з грифом секретності «Особливо важливо», «Цілком таємно», «Таємно», яка циркулює в підсистемі ОВУ. Для розрахунку коефіцієнту захищеності інформації, що становить ДТ *($K_{з\ і}$)* обрані такі визначення:

Перелік відомостей i, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ:

$$i = \{i_1, i_2, \ldots, i_a, \ldots, i_n\},\ a = \overline{1, N}, \quad (1)$$

де i – перелік статей ЗВДТ, що належать до компетенції сектору оборони України;

N – кількість статей ЗВДТ;

i_a – відомості, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ.

Перелік коефіцієнтів важливості β відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ:

$$\beta = \{\beta_1, \beta_2, \ldots, \beta_a, \ldots, \beta_n\}, a = \overline{1, N}, \quad (2)$$

де β – коефіцієнт важливості відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ;

β_a – коефіцієнт важливості N-х відомостей, що підпадають під дію статей ЗВДТ і циркулюють в підсистемі ОВУ.

β_N – коефіцієнт важливості відомостей, що підпадають під дію статей ЗВДТ і циркулюють в підсистемі ОВУ, розраховується відповідно до шкоди, що заподіяна органам військового управління внаслідок витоку секретної інформації або втрати матеріальних носіїв секретної інформації (далі – МНСІ).

Перелік загроз захищеності H відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ:

$$H = \{h_1, h_2, \ldots, h_b, \ldots, h_u\},\ b = \overline{1, u}, \quad (3)$$

де h_b – b-ая загроза захищеності відомості i_a, що належить до відомостей з інформацією, яка становить ДТ і циркулює в підсистемі ОВУ;

u – кількість загроз захищеності N відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ. У загальному випадку $N \neq u$.

Перелік загроз (несанкціонований доступ, виток секретної інформації або втрата МНСІ) для секретної інформації, яка циркулює в підсистемі ОВУ визначається за допомогою матриці загроз, що складається за експертними оцінками.

Перелік узагальнених коефіцієнтів важливості загроз захищеності L відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ*:*

$$L = \{L_b\},\ b = \overline{1, u}, \quad (4)$$

де L_b – узагальнюючий коефіцієнт важливості b-ої загрози захищеності секретної інформації, що циркулює в підсистемі ОВУ.

Для розрахунку узагальнюючого коефіцієнту важливості L_b, використовується матриця F взаємозв'язку інформації, що становить державну таємницю i_a з загрозами захищеності h:

$$F = ||f_{ab}||_{N,u}, \quad (5)$$

Кожний елемент матриці визначається згідно з виразом:

$$f_{ab} \begin{cases} 0, \text{ якщо } h_b \overline{\in} H_a \\ \mathcal{L}_{ab}, \text{ якщо } h_b \in H_a \end{cases} \quad (6)$$

де H_a – множина загроз ($H_a \in H$) захищеності відомостей, що становлять ДТ i_a й циркулюють в підсистемі ОВУ;

l_{ab} – значення коефіцієнта важливості загрози h_b захищеності відомостей, що становлять ДТ i_a й циркулюють в ОВУ.

За обчислення l_{ab} враховуються коефіцієнти важливості відомостей β_N так, щоб виконувалась умова:

$$\sum_{h_b \in H_a} l_{ab} = \beta_a, \quad (7)$$

де l_{ab} визначається з урахуванням виразу:

$$l_a = \beta_a / |H_a|,\ a = \overline{1, N}, \quad (8)$$

де $|H_a|$ – кількість загроз у множині H_a.

За умов, визначених виразами (4, 5, 6, 7, 8), коефіцієнти важливості загроз захищеності L відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ, можна навести у вигляді:

$$L = J_N \cdot F, \quad (9)$$

де $L = ||L_1, L_2, \ldots, L_a, \ldots, L_u||$ – вектор-рядок коефіцієнтів важливості загроз захищеності відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ;

L_a – узагальнюючий (сумарний) коефіцієнт важливості загрози h_b характеризує важливість усунення загрози h_b з урахуванням сумарної кількості й важливості відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ, для яких існує ця загроза;

J_N – вектор-рядок, який складається з N (кількості статей ЗВДТ), кожен з яких дорівнює 1;

F – матриця взаємозв'язку i (перелік статей ЗВДТ), з H (перелік загроз захищеності відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ), має вигляд:

$$F = \begin{vmatrix} f_{11} & f_{12} & \cdots & f_{1n} & f_{1,u} \\ f_{21} & f_{22} & \cdots & f_{2,n} & f_{2,u} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ f_{N,1} & f_{N,2} & & f_{N,n} & f_{N,u} \end{vmatrix}, \quad (10)$$

Остаточно з виразу (6) отримаємо:

$$\begin{matrix} L_1 = f_{11} + f_{12} + \ldots + f_{1n} + \ldots + f_{1u} \\ L_2 = f_{21} + f_{22} + \ldots + f_{2n} + \ldots + f_{2u} \\ \ldots = \ldots + \ldots + \ldots + \ldots + \ldots + \ldots \\ L_N = f_{N1} + f_{N2} + \ldots + f_{Nn} + \ldots + f_{Nu} \end{matrix}, \quad (11)$$

Перелік завданъ S з усунення загроз захищеності відомостей, що містять інформацію, яка становить державну таємницю і циркулює в підсистемі ОВУ:

$$S = \{s_g\},\ g = 1,\ e, \quad (12)$$

де s_g – g-е завдання стосовно усунення загроз захищеності секретних відомостей, що циркулюють у підсистемі ОВУ;

e – кількість завдань з усунення загрози секретних відомостей, що циркулюють в підсистемі ОВУ. Формування переліку завдань щодо усунення загроз захищеності відомостей здійснюється експертним методом.

Завдання s_g впорядковуються за місцем і часом їх вирішення, якщо це потрібно. В завданнях s_g формулюються такі позиції: спосіб усунення загроз (розмежування доступу до секретної інформації, проведення технічних заходів захисту секретної інформації та інше); сама загроза, що підлягає усуненню; період часу, протягом якого загрозу захищеності відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ, необхідно усунути.

Множина завдань S у варіанті задуму усунення загрози захищеності відомостей, що містять секретну інформацію, яка циркулює в підсистемі ОВУ, має бути достатньою для захисту кожного елементу відомостей $i_a \in i$ від кожної загрози $h_b \in H$, але, за можливості, мінімальною.

Перелік заходів T з усунення загроз захищеності відомостей, які містять інформацію, що становить ДТ і циркулює в підсистемі ОВУ:

$$T = \{t_k\},\ k = \overline{1, e}, \quad (13)$$

де t_k – захід, який забезпечує виконання g-го завдання S_g з усунення загрози захищеності окремих i_a відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ.

Заходи обираються відповідно до переліку організаційно-правових, технічних, криптографічних та оперативно-розшукових заходів, визначених в [1] та інших нормативних документів, що регламентують порядок класифікації, засекречування та доступ до секретної інформації в підсистеи ОВУ.

Захід t_k усунення загрози захищеності окремих секретних відомостей визначається для кожного завдання S_k . Порівнянням можливих засобів і способів розв'язання завдання захисту відомостей, що містять секретну інформацію, обираються найбільш ефективні з них.

Перелік P_k ймовірностей усунення загроз захищеності відомостей, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ:

$$P_k = \{P(h_b/t_k)\},\ k = \overline{1, e}, \quad (14)$$

де $P(h_b/t_k)$ – показник захищеності k-го заходу з усунення b-ої загрози захищеності окремої секретної відомості. Цей показник розраховується для кожного заходу за допомогою експертних комісій при Державному експерті з питань таємниці [1]. Він характеризує ефективність k-го заходу за умови виконання відповідного завдання з усунення загрози захищеності секретної інформації, що циркулює в підсистемі ОВУ і має ймовірнісний характер.

Показники захищеності комплексу заходів з усунення загрози відомостям, що містять інформацію, яка становить ДТ і циркулює в підсистемі ОВУ:

Усунення однієї загрози h_b, загалом, забезпечується за умов реалізації декількох завдань захисту секретних відомостей. Припустимо, що сукупність заходів з нейтралізації певної b-ої загрози може виконуватись одночасно. Визначимо ці заходи як $t_g,\ldots,t_q$ ймовірність усунення кожним із них загрози h_b, через $P(h_b/t_g),\ldots,P(h_b/t_q)$.

Ймовірність того, що загроза h_b не буде нейтралізована окремо кожним із цих заходів, обчислюється за виразом:

$$\bar{P}\,(h_b/t_k) = 1 - P\,(h_b/t),\ k = g,\ldots q \quad (15)$$

Ймовірність того, що загроза h_b існуватиме попри реалізацію всієї сукупності заходів, тобто остатня ймовірність існування загрози після введення системи забезпечення захисту секретної інформації, визначається як:

$$P\,(h_b/t_g,\ldots,t_q) = \prod_{k=g,\ldots q} 1 - P\,(h_b/t_k) \quad (16)$$

Ймовірність нейтралізації загрози h_b сукупною дією усіх заходів $t_g,\ldots,t_q$ обчислюється виразом:

$$P(h_b/t_g,..,t_q) = 1 - \bar{P}(h_b/t_g,..,t_q) = 1 - \prod_{k=g,..q} 1 - P(h_b/t_k) \quad (17)$$

За результатом обчислень складається вектор-рядок P значень $P(h_b)$ показників ефективності усунення відповідних загроз h_b:

$$P = \|P_1, P_2, \ldots P_b, \ldots P_u\|, \quad (18)$$

де ймовірність нейтралізації b-ої загрози скорочено позначено через P_b, $b = \overline{1, u}$.

Етап формування вихідних даних відомостей, що містять інформацію, яка становить державну таємницю і циркулює в підсистемі ОВУ, завершено.

Розглянемо наступний етап 1 Блоку. Формування вихідних даних СлІ з грифом обмеження «Для службового користування», що циркулює в підсистемі ОВУ. Для визначення коефіцієнту захищеності СлІ, що ($K_{з\ j}$) обрані такі показники:

Перелік відомостей j, що містять інформацію, яка становить СлІ і циркулює в підсистемі ОВУ:

$$j = \{j_1, j_2, ..., j_a, ..., j_m\},\ a = \overline{1, M}, \quad (19)$$

де j – перелік пунктів ПСІ, що належать до компетенції сектору оборони України;

M – кількість пунктів ПСІ;

j_a – відомості, що містять СлІ і циркулюють в підсистемі ОВУ.

Перелік коефіцієнтів важливості Λ відомостей, що містять СлІ і циркулюють в підсистемі ОВУ:

$$\Lambda = \{\Lambda_1, \Lambda_2, ..., \Lambda_a, ..., \Lambda_m\},\ a = \overline{1, M}, \quad (20)$$

де Λ – коефіцієнт важливості відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ;

Λ_a – коефіцієнт важливості M-их відомостей СлІ, які підпадають під дію пунктів ПСІ, що циркулюють в підсистемі ОВУ.

Λ_M – коефіцієнт важливості відомостей СлІ, які підпадають під дію пунктів ПСІ, що циркулюють в підсистемі ОВУ розраховується відповідно до шкоди, що заподіяна органу військового управління внаслідок витоку СлІ або втрати МНІ.

Перелік загроз захищеності R відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ:

$$R = \{r_1, r_2, ..., r_b, ..., r_u\},\ r = \overline{1, u}, \quad (21)$$

де r_b – b-ая загроза захищеності відомості j_a, що належить до відомостей, які містять СлІ і циркулюють в підсистемі ОВУ;

u – кількість загроз захищеності M відомостей, що містять СлІ і циркулюють в підсистемі ОВУ. Загалом $M \neq u$.

Перелік загроз (несанкціонований доступ, виток інформації або втрата МНІ) для СлІ, що циркулює в підсистемі ОВУ визначається за допомогою матриці загроз, яка складається за експертними оцінками.

Перелік узагальнених коефіцієнтів важливості загроз захищеності V відомостей, що містять СлІ й циркулюють в підсистемі ОВУ:

$$V = \{V_b\},\ b = \overline{1, u}, \quad (22)$$

де V_b – узагальнюючий коефіцієнт важливості b-ої загрози захищеності СлІ, що циркулює в підсистемі ОВУ.

Для розрахунку узагальнюючого коефіцієнту важливості V_b, використовується матриця F взаємозв'язку службової інформації j_a із загрозами захищеності r:

$$F = ||f_{ab}||_{M,u}, \quad (23)$$

Кожний елемент матриці визначається згідно з виразом:

$$f_{ab} \begin{cases} 0, \text{ якщо } r_b \overline{\in} R_a \\ \mathcal{L}_{ab}, \text{якщо } r_b \in R_a \end{cases} \quad (24)$$

де R_a – множина загроз ($R_a \in R$) захищеності відомостей, що містять СлІ j_a і циркулюють в підсистемі ОВУ;

v_{ab} – значення коефіцієнта важливості загрози r_b захищеності відомостей, що містять СлІ j_a і циркулюють в ОВУ.

Під час обчислення v_{ab} враховуються коефіцієнти важливості відомостей Λ_M так, щоб виконувалась умова:

$$\sum_{r_b \in R_a} v_{ab} = \Lambda_a, \quad (25)$$

де v_{ab} визначається враховуючи вираз:

$$v_{ab} = \Lambda_a / |R_a|,\ a = \overline{1, M}, \quad (26)$$

де $|V_a|$ – кількість загроз у множині V_a.

За умов, що визначені виразами (22, 23, 24, 25, 26), коефіцієнти важливості загроз захищеності V відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ, можуть бути наведені виразом:

$$L = J_M \cdot R, \quad (27)$$

де $L = ||L_1, L_2, ..., L_a, ..., L_u||$ – вектор-рядок коефіцієнтів важливості загроз захищеності відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ;

V_a – узагальнюючий коефіцієнт важливості загрози r_b. Він характеризує важливість усунення загрози r_b з урахуванням сумарної кількості й важливості відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ, для яких існує така загроза;

J_M – вектор-рядок, який складається з M (кількості пунктів ПСІ), кожен з яких дорівнює 1;

F – матриця взаємозв'язку і (перелік пунктів ПСІ) з V (перелік загроз захищеності відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ) має вигляд:

$$F = \begin{vmatrix} f_{11} & f_{12} & \cdots & f_{1m} & f_{1,u} \\ f_{21} & f_{22} & \cdots & f_{2,m} & f_{2,u} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ f_{M,1} & f_{M,2} & & f_{M,m} & f_{M,u} \end{vmatrix}, \quad (28)$$

Остаточно з виразу (24) отримаємо:

$$\begin{matrix} L_1 = f_{11} + f_{12} + \ldots + f_{1m} + \ldots + f_{1u} \\ L_2 = f_{21} + f_{22} + \ldots + f_{2m} + \ldots + f_{2u} \\ \ldots = \ldots + \ldots + \ldots + \ldots + \ldots + \ldots \\ L_M = f_{M1} + f_{M2} + \ldots + f_{Mm} + \ldots + f_{Mu} \end{matrix}, \quad (29)$$

Перелік завданъ D з усунення загроз захищеності відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ:

$$D = \{d_g\},\ g = 1,\ e, \quad (30)$$

де d_g – g-е завдання щодо усунення загроз захищеності відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ;

e – кількість завдань з усунення загрози відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ. Формування переліку завдань щодо усунення загроз захищеності відомостей здійснюється експертним методом.

Завдання d_g впорядковуються за місцем і часом їх вирішення, якщо це потрібно. В завданнях d_g формулюються такі позиції: спосіб усунення загрози (розмежування доступу до СлІ, проведення технічних заходів захисту СлІ та інше); сама загроза, що підлягає усуненню; період часу, протягом якого загрозу захищеності відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ, необхідно усунути.

Множина завдань D у варіанті задуму усунення загрози захищеності відомостей, що містять СлІ і циркулюють в підсистемі ОВУ, має бути достатньою для захисту кожного елементу відомостей $j_a \in j$ від кожної загрози $r_b \in R$, але, за можливості, мінімальною.

Перелік заходів T з усунення загроз захищеності відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ:

$$T = \{t_k\},\ k = \overline{1, e}, \quad (31)$$

де t_k – захід, який забезпечує виконання g-го завдання D_g з усунення загрози захищеності окремих j_a відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ.

Вибір заходів здійснюється згідно з передбаченим законом переліком організаційно-правових, технічних та оперативно-розшукових заходів, які визначені у [2] та іншими нормативними документами, що регламентують порядок ведення обліку, зберігання, використання і знищення документів та інших МНІ, що містять СлІ в підсистеии ОВУ.

Захід t_k усунення загрози захищеності окремих відомостей, що містять службову інформацію визначається для кожного завдання D_k . Порівнянням можливих засобів і способів розв'язання завдання захисту відомостей, що містять службову інформацію обираються найбільш ефективні з них.

Перелік P_k ймовірностей усунення загроз захищеності відомостей, що містять СлІ і циркулюють в підсистемі ОВУ:

$$P_k = \{P(r_b/t_k)\},\ k = \overline{1, e}, \quad (32)$$

де $P(h_b/t_k)$ – показник захищеності k-го заходу з усунення b-ої загрози захищеності окремої службової відомості.

Показник $P(r_b/t_k)$ розраховується для кожного заходу на підставі пропозицій, підготовлених постійно діючою комісією з питань роботи із СлІ в Міністерстві оборони України та Генерального Штабу ЗС України [14]. Цей показник характеризує захищеність k-го заходу за умови виконання відповідного завдання з усунення загрози захищеності СлІ, яка циркулює в підсистемі ОВУ і має імовірнісний характер.

Показники захищеності комплексу заходів з усунення загрози відомостям, що містять СлІ, яка циркулює в підсистемі ОВУ:

усунення однієї загрози r_b, загалом, забезпечується за умов реалізації декількох завдань захисту відомостей, що містять СлІ.

Припустимо, сукупність заходів з нейтралізації певної b-ої загрози може виконуватись одночасно. Визначимо ці заходи як t_g ,...,t_q ймовірність усунення кожним із них загрози κ_b, через $P(r_b/t_g)$,...,$P(r_b/t_q)$. Ймовірність того, що загроза r_b не буде нейтралізована окремо кожним з цих заходів обчислюється за виразами:

$$\bar{P}\,(r_b/t_k) = 1 - P\,(rh_b/t)\,,\ k = g, \ldots q \quad (33)$$

Ймовірність того, що загроза r_b існуватиме попри реалізацію всієї сукупності заходів, тобто апостеріорна ймовірність існування загрози після введення системи забезпечення захисту інформації, визначається як:

$$P\,(r_b/t_g, \ldots, t_q) = \prod_{k=g,\ldots q} 1 - P\,(r_b/t_k) \quad (34)$$

Ймовірність нейтралізації загрози r_b сукупною дією усіх заходів $t_g, \ldots, t_q$ обчислюється виразом:

$$P(r_b/t_g, .., t_q) = 1 - \bar{P}(r_b/t_g, .., t_q) = 1 - \prod_{k=g,\ldots q} 1 - P(r_b/t_k) \quad (35)$$

За результатом обчислень складається вектор-рядок P значень $P(r_b)$ показників ефективності усунення відповідних загроз r_b:

$$P = \|P_1, P_2, \ldots P_b, \ldots P_u\|, \quad (36)$$

де ймовірність нейтралізації b-ої загрози скорочено позначено через P_b, $b = 1, u$.

Етап формування вихідних даних відомостей, що містять СлІ, яка циркулює в підсистемі ОВУ завершено. Всі вихідні данні заносяться у «Перелік можливих заходів щодо усунення загроз захищеності відомостей, що містять ІзОД і показників їх ефективності» на підставі якого

здійснюється розрахунок $K_{з\ i,j}$ коефіцієнту захищеності ІзОД наведений в *2 Блоці* удосконаленої методики.

2 Блок. На підставі сформованих вихідних даних ІзОД, яка циркулює в підсистемі ОВУ системи управління ОУВ(с), можна визначити $K_{з\ i,j}$ коефіцієнт захищеності ІзОД. Коефіцієнт характеризує ступінь зниження можливих втрат, які обумовлені витоком ІзОД та втратам МНІ.

Розрахунок коефіцієнта захищеності ІзОД $K_{з\ i,j}$. З урахуванням ступеня усунення загроз захищеності ІзОД, яка підпадає під дії статей ЗВДТ (*i)* та пунктів ПСІ (*j*), що циркулюють в ОВУ та підлягають захисту, а також коефіцієнтів важливості загроз захищеності *L* (відомостей, що містять інформацію, яка становить ДТ) та *V* (відомостей, що містять СлІ), визначається коефіцієнт захищеності відомостей, що відносяться до ІзОД:

$$K_{з\ i} = L \cdot P(h_i), \tag{37}$$

$$K_{з\ j} = V \cdot P(r_j), \tag{38}$$

де *L, V* – вектора-рядки значень коефіцієнтів важливості загроз захищеності ІзОД, що циркулює в підсистемі ОВУ;

P – вектор-рядок значень показників ефективності усунення відповідних загроз h_i, r_j.

Слід зазначити, що за визначення ефективності функціонування СЗЗІзОД в конкретному ОУВ(с) підсистеми ОВУ потреба в обрахуванні сукупності коефіцієнтів $K_{з\ i,j}$ більше не виникає.

В цьому випадку множина коефіцієнтів важливості (*L* (вираз (4) та *Λ* (вираз (22)) буде складатися з усіх відомостей з обмеженим доступом, що циркулюють в конкретному ОУВ(с) підсистеми ОВУ. Для них визначається загальний перелік загроз й певна сукупність заходів з їх нейтралізації, відповідно до чого розраховуються вектори *L, Λ* і $P(h_i), P(r_j)$ безпосередньо за якими обчислюється коефіцієнт захищеності СЗЗІзОД для ОУВ(с):

$$K^{СЗЗІзОД} = (L \cdot Λ) \cdot (P(h_i) \cdot P(r_j), \tag{39}$$

3 Блок. Для визначення потенційної шкоди Wij ОУВ(с) в підсистемі ОВУ за витоку ІзОД або втрати МНІ використовується шкала оцінювання.

Для відомостей які містять інформацію, що становить ДТ на підставі *i*-ої статті ЗВДТ доцільно використовувати трирівневу шкалу оцінювання. Значення шкали оцінювання знаходиться у межах від 1 до 100. Згідно з цією шкалою для різних ступенів секретності інформації пропонується використовувати такі значення показника W_i:

«Таємно» – інтервал $1 \leq W_{Ti} < 10$, з середнім інтервальним значенням $W_{Ti} = 5$;

«Цілком таємно» – інтервал $10 \leq W_{ЦТi} < 50$, з середнім інтервальним значенням $W_{ЦТi} = 30$;

«Особливої важливості» – інтервал $50 \leq W_{OBi} \leq 100$, з середнім інтервальним значенням $W_{OBi} = 75$.

Для відомостей які містять СлІ та підпадають під дію *j*-го пункту ПСІ, значення оцінювання знаходиться у межах від 1 до 10. «Для службового користування» – інтервал $1 \leq W_{ДСКj} \leq 10$, з середнім інтервальним значенням $W_{ДСКj} = 5$;

Потенційна сукупна шкода є ключовим параметром, який впливає на методику оцінювання захищеності ІзОД та вибір заходів з усунення загроз захищеності відомостей, що циркулюють в ОУВ(с) підсистеми ОВУ.

$$W_з^{ОВУ} = \sum_{i,j=1}^{N,M} W_{i,j}, \tag{40}$$

Залежно від рівня шкоди, система може вміщувати додаткові організаційно-правові, технічні та оперативно-розшукові заходи.

4 Блок. Проводиться розрахунок коефіцієнта захищеності ІзОД в ОВУ $K_з^{ОВУ}$.

В цьому випадку множина *β* та *Λ* вирази (2, 20) буде складатися з коефіцієнтів важливості усіх відомостей ІзОД, яка циркулює в підсистемі ОВУ системи управління ОУВ(с), без поділу на інформацію, що становить ДТ та СлІ. Для цих відомостей визначається загальний перелік загроз й певна сукупність заходів з їх нейтралізації, відповідно до чого розраховуються вектори *L*, *V* та $P(h_i) \cdot P(r_j)$, безпосередньо за якими обчислюється коефіцієнт захищеності ІЗОД $K_з^{ОВУ}$, що характеризує ступінь ефективності функціонування СЗЗІзОД в підсистемі ОВУ під час виконання операцій в зоні проведення бойових дій.

У такій ситуації немає потреби в оцінці потенційної сукупної шкоди $W_{i,j}$ заподіяної витоком ІзОД або втратою МНІ. Це наведено у виразі:

$$К_З^{ОВУ} = W_Р \ / W_{i,j}, \tag{41}$$

де W_p – шкода для підсистеми ОВУ з урахуванням реального стану СЗЗІзОД.

Через відсутність поділу ІзОД на ДТ та СлІ *N, M* = 1, $K_з^{ОВУ}$ обчислюється за формулою:

$$K_з^{ОВУ} = \frac{\sum_{i,j=1}^{N\ M}(W_{i,j} * K_{зi,j})}{\sum_{i,j=1}^{N\ M}(W_{i,j})}, \tag{42}$$

5 Блок. Розрахунок коефіцієнта захищеності $K_з^{ОВУ}$ *ефективного функціонування СЗЗІзОД в підсистемі ОВУ системи управління ОУВ(с).*

Обчисливши сукупність показників загальної потенційної шкоди для підсистеми ОВУ за формулою (40), розрахуємо можливості ефективного функціонування системи забезпечення захисту інформації, у разі повної захищеності ІзОД за формулою:

$$W_р^{ОВУ} = \sum (W_{i,j} \cdot К_{Зi,j}), \tag{43}$$

де *i, j = 1, NM* за умов реального стану системи забезпечення захисту ІзОД в підсистемі ОВУ системи управління ОУВ(с) під час здійснення операцій у районі бойових дій, згідно виразу:

$$K_{\text{з}}^{\text{ОВУ}} = \frac{\sum_{i,j=1}^{N,M}(W_{i,j} * K_{\text{з}i,j})}{\sum_{i,j=1}^{N,M}(W_{i,j})}, \quad (44)$$

Отримуємо кількісну оцінку коефіцієнта захищеності ІзОД в підсистемі ОВУ.

Оцінювання захищеності ІзОД в підсистемі ОВУ проводиться за рівнем достатності, шляхом порівняння розрахункових значень $K_{\text{з}}^{\text{ОВУ}}$ з тим, що потрібно. Водночас, широко застосовують експертний та сценарний метод. Результати проведених досліджень із оцінювання захищеності дають змогу сформувати класифікацію коефіцієнта захищеності ІзОД.

Для переходу від якісного до кількісного оцінювання коефіцієнта застосовується безрозмірна шкала бажаності Харінгтона, розроблена автором із використанням [13] (табл. 1).

Таблиця 1

Безрозмірна шкала бажаності Харінгтона

Лінгвістична оцінка		*Інтервали числових значень рівня захисту інформації* $K_{\text{з}}^{\text{ОВУ}}$
За типовою шкалою Харрінгтона	*За шкалою, адаптованою до змісту задачі оцінювання захищеності ІзОД в підсистемі ОВУ,* $K_{\text{з}}^{\text{ОВУ}}$ *(вербальна характеристика)*	
Дуже добре	*Високий – відповідність заходам безпеки* (система забезпечення захисту ІзОД в ОВУ відповідає встановленим вимогам і забезпечує високий рівень безпеки інформації, зводячи ймовірність витоку ІзОД та втрати матеріальних носіїв інформації до мінімуму). Система забезпечена повністю, можливості витоку інформації або втрати МНІ практично не існує.	*1,00-0,80* $K_{\text{з}}^{\text{ОВУ}} \geq 0,80$
Добре	*Вище середнього – загалом відповідає встановленим заходам безпеки,* однак ефективність функціонування системи забезпечення захисту ІзОД в ОВУ вимагає оцінювання захищеності інформації для своєчасного виявлення і усунення потенційних загроз. Система забезпечена у цілому, але є можливість витоку інформації або втрати МНІ	*0,80-0,63* $0,8 > K_{\text{з}}^{\text{ОВУ}} > 0,63$
Задовільно	*Середній – система частково відповідає встановленим заходам безпеки*, однак ефективність її функціонування є обмеженою. Виявлені недоліки можуть впливати на зниження загального рівня захищеності. Необхідне доопрацювання окремих завдань з усунення загроз захищеності ІзОД в системи для забезпечення її повної відповідності вимогам. Недостатнє впровадження або застарілість окремих заходів безпеки. Частина загроз може залишатися нерозпізнаною через обмежені можливості спостереження. Регулярний аналіз та оновлення заходів безпеки для досягнення повної відповідності до встановлених вимог.	*0,63-0,37* $0,63 > K_{\text{з}}^{\text{ОВУ}} > 0,37$
Погано	*Нижче середнього – неефективність заходів* (призведуть до нездатності системи забезпечення захисту ІзОД ефективно запобігти загрозам, які можуть вплинути на функціонування ОВУ). Система має суттєві недоліки у функціонуванні та захищеності інформації, що збільшує ризик реалізації загроз. Впроваджені заходи неефективні або виконуються неповністю. Частина вимог стосовно захищеності ІзОД не виконується, що робить систему забезпечення захисту інформації вразливою до несанкціонованого доступу. Велика кількість потенційних загроз залишається невиявленою або неусунутою. Невідкладне проведення оцінювання системи із подальшим посиленням захисту шляхом впровадження додаткових організаційно-правових і технічних заходів.	*0,37-0,20* $0,37 > K_{\text{з}}^{\text{ОВУ}} > 0,2$
Дуже погано	*Низький – система забезпечення захисту ІзОД практично не відповідає встановленим вимогам*, що створює критичну загрозу для безпеки інформації. Відсутність належних технічних і організаційних заходів, слабкий контроль доступу, неефективність аналізу й управління. Ймовірність витоку інформації або втрати матеріальних носіїв є дуже високою. Проведення комплексного аналізу загроз і термінове впровадження заходів захисту ІзОД для досягнення мінімально прийнятного рівня безпеки.	*0,2-0,00* $K_{\text{з}}^{\text{ОВУ}} \leq 0,2$

Оцінювання засвідчило, що коефіцієнт захищеності ІзОД перевищує значення $K_{\text{з}}^{\text{ОВУ}} \geq 0,80$, що вказує на високий рівень відповідності СЗЗІзОД встановленим вимогам безпеки інформації. СЗЗІзОД в ОУВ(с) функціонує ефективно, зводячи до мінімуму ймовірність витоку інформації або втрати МНІ. Досягнення такого рівня захищеності є результатом належного впровадження технічних, організаційно-правових та оперативно-розшукових заходів. Усі необхідні умови виконані, що забезпечує повну відповідність системи.

6 Блок. На підставі розрахунку коефіцієнта захищеності ІзОД його числових значень $K_{\text{з}}^{\text{ОВУ}} \geq 0,80$ менших за 0,8. Нездатність СЗЗІзОД

ефективно запобігти загрозам, що можуть вплинути на функціонування ОУВ(с) та виявлення причин невідповідності визначеним вимогам.

7 Блок. Проведення невиконаних заходів та впровадження додаткових технічних, організаційно-правових і оперативно-розшукових дій з метою забезпечення належного рівня захисту ІзОД. Аналіз загроз, виявлення порушень вимог безпеки інформації та надання пропозицій щодо підвищення ефективності функціонування СЗЗІзОД в умовах здійснення операцій ОУВ(с) у районах бойових дій, дасть змогу унеможливити виток інформації або втрату МНІ, мінімізувати ризики, пов'язані з впливом загроз безпеці інформації, а також забезпечити оперативність та надійність прийняття рішень командуванням у критичних умовах.

8. Підсумки. Удосконалена методика оцінювання захищеності ІзОД, яка циркулює в підсистемі ОВУ, дає змогу визначити рівень безпеки інформації відповідно до встановлених вимог. Проведений аналіз підтверджує, що СЗЗІзОД в ОУВ(с) забезпечує високий рівень безпеки, мінімізуючи ймовірність витоку інформації або втрати МНІ.

Результати оцінювання свідчать про повну відповідність СЗЗІзОД встановленим стандартам, що унеможливлює виникнення суттєвих ризиків. Це досягається завдяки впровадженню комплексних заходів безпеки, які охоплюють технічний, організаційно-правовий та оперативно-розшуковий компоненти. Використання даної методики дає змогу не лише підтримувати високий рівень захищеності інформації, а й своєчасно виявляти потенційні загрози та удосконалювати заходи безпеки відповідно до змін у характері загроз.

Висновки й перспективи подальших досліджень

Результати проведеного наукового дослідження підтвердили досягнення поставленої мети – вдосконалення методики оцінювання захищеності інформації з обмеженим доступом, яка циркулює в підсистемі органів військового управління, що здійснене для запобігання витоку інформації та недопущення втрати її матеріальних носіїв й унеможливлення використання цих відомостей противником.

Запропоноване вдосконалення методики дає змогу забезпечити надійний рівень захищеності інформації, запобігти її витоку та втраті, мінімізувати ризики та адаптувати підходи до оцінювання захищеності з урахуванням сучасних загроз, високої динаміки ведення бойових дій і потреб в секторі оборони України.

Теоретична значущість дослідження зводиться до створення нових концептуальних основ для оцінювання захищеності інформації з обмеженим доступом, які враховують сучасні виклики та оперативну обстановку. Практичною цінністю вдосконаленої методики є її здатність забезпечувати своєчасне виявлення загроз, підвищувати ефективність заходів із їх усунення та гарантувати стабільне функціонування системи управління військами в умовах інтенсивних бойових дій.

Розроблена система забезпечення захисту інформації з обмеженим доступом забезпечує надійну передачу даних, оперативну координацію дій та ухвалення рішень у реальному часі, що є визначальним для успішного виконання бойових завдань.

Перспективними напрямами подальших досліджень є: аналіз практичного застосування методики для удосконалення процедур ухвалення рішень в умовах обмеженого часу; розробка нових показників оцінювання ефективності заходів захисту інформації з обмеженим доступом з урахуванням специфіки бойових завдань; вдосконалення нормативно-правової бази для посилення спроможності органів військового управління забезпечувати захист інформації з обмеженим доступом; інтеграція сучасних технологій у процеси оцінювання та забезпечення захищеності інформації з обмеженим доступом; реалізація програмного продукту, що визначатиме рівень завданої шкоди органу військового управління у разі витоку інформації або втрати відомостей, за допомогою об'єктивних знань на основі нейронної мережі (штучного інтелекту) та експертної оцінки Державного експерта з питань таємниць; дослідження впливу нових загроз безпеки інформації на функціонування підсистем органів військового управління в умовах війни. Отримані результати створюють основу для подальших наукових розробок у сфері безпеки інформації та підвищення ефективності функціонування системи управління військами.

Список бібліографічних посилань

1. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. URL: https://www.zakon.rada.gov.ua/laws/show/ 3855-12 (дата звернення: 22.11.2024). **2. Про інформацію** : Закон України від 02.10.1992 № 2657-XII. URL: https://www.zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 22.11.2024). **3. Звід відомостей**, що становлять державну таємницю : Наказ Служби безпеки України від 23.12.2020 № 383. URL: https://www.zakon.rada.gov.ua/ laws/show/z0052-21 (дата звернення: 22.11.2024). **4. Перелік** відомостей Міністерства оборони України, які містять службову інформацію : Наказ Міністерства оборони України від 17.10.2023 № 605. URL: https://www.zakon.rada.gov.ua/ rada/show/v0605322-23 (дата звернення: 22.11.2024). **5. Стратегія** національної безпеки України : Указ Президента України від 26.05.2015 № 287/2015. URL: https://www.zakon.rada.gov.ua/laws/show/287 (дата звернення: 22.11.2024). **6. Політика безпеки НАТО** (С-М(2002)49). Адміністративні домовленості : Закон

України від 24.05.2017 № 2068-VIII. URL: https://www.uvns.hr/UserDocsImages/Nato (дата звернення: 22.11.2024). **7. Правила безпеки ЄС** 2013/488/EU Council security rules for protecting classified information (EUCI) Council Decision of 23.09.2013 on the security rules for protecting EU classified information. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013 D0488 (дата звернення: 22.11.2024). **8. Про безпеку класифікованої інформації** : Законопроєкт Верховної Ради України від 27.01.2023 № 8394. URL: https://www.itd.rada.gov.ua/billInfo/Bills/Card/41249 (дата звернення: 22.11.2024). **9. Вдовенко С. Г.** Сучасні вимоги до охорони державної таємниці та захисту інформації з обмеженим доступом в особливий період. *Імперативи розвитку цивілізації*. 2015. № 2. С. 93–96. **10. Шкарлат О. О., Штонда Р. М., Сулімовська М. В.** Захист інформації в автоматизованих системах суб'єктів охоронної діяльності. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2018. № 2(32). С. 17–22. **11. Вдовенко С. Г., Гулак Ю. С., Машталір В. В.** Законодавчі, нормативно-правові та дефініційні аспекти проблем у сфері охорони державної таємниці та службової інформації в умовах війни та шляхи їх вирішення. *Актуальні проблеми інформаційної безпеки держави* : Матеріали XIV Всеукраїнської наук.-практ. конф., 30 березня 2023 року, м. Київ. 2023. **12. Болдир С. В.** Перспективи реформування системи охорони державної таємниці та службової інформації. *Інформація і право*. 2017. № 4(23). **13. Корченко О. Г., Архіпов О. Є., Дрейс Ю. О.** Оцінювання шкоди національній безпеці України в разі витоку державної таємниці : монографія. НА СБ України, Київ, 2014. С. 206–213. **14. Типова інструкція** про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, ПКМ України від 19.10.2016 № 736 Київ. URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text (дата звернення: 22.11.2024).

AN ADVANCED METHODOLOGY FOR ASSESSING THE SECURITY OF RESTRICTED INFORMATION CIRCULATING IN THE SUBSYSTEM OF MILITARY COMMAND AND CONTROL BODIES

Sulimovska Mariia

National Defence University of Ukraine, Kyiv, Ukraine

Formulation of the problem in general. *The article formulates a current challenge of assessing the security of classified information circulating in the subsystem of military command and control bodies of the command and control system of an operational group of troops (forces) during operations in the combat zone and proposes a solution to this problem. The analysis of the functioning of an operational grouping of troops (forces) confirms that this problem is relevant and needs to be solved in the context of the large-scale armed aggression of the russian federation against Ukraine. The purpose of the article is to develop an improved methodology for assessing the security of restricted information circulating in the subsystem of military command and control bodies with a view to preventing information leakage, preventing loss of its material storage media and making it impossible for the enemy to use this information.*

Research methods: *system analysis, modelling method, expert assessments, comparative analysis method, SWOT analysis method, statistical analysis method, scenario analysis method. This methodological approach made it possible to properly assess the security of restricted information.*

The analysis of research and publications *on information security assessment shows that it needs to be updated and improved, taking into account the security threats caused by the high dynamics of hostilities.*

Presenting the main material *The article shows that solving this problem requires a systematic approach and effective application of indicators for assessing the security of restricted information in the subsystem of military command and control bodies. Proposes to define the coefficient of security of restricted information, which characterises the degree of efficiency of the information security system in the subsystem of military command and control bodies during operations. This indicator is limited to the articles of the Code of Information Constituting a State Secret and the items of the List of Official Information belonging to the structures of the defence sector of Ukraine (the Armed Forces of Ukraine and the Ministry of Defence of Ukraine). The advanced methodology for assessing the security of restricted information consists of eight blocks, including the generation of initial data, the calculation of security coefficients and the assessment of potential damage from information leakage or loss of data. The methodology also includes identifying the causes of non-compliance, developing recommendations to improve the effectiveness of protection and determining the overall level of information security. Its implementation helps to ensure that the system for protecting restricted information in the subsystem of military command and control bodies meets the established requirements and minimises the risk of loss of material information carriers.*

The scientific novelty *is the introduction of a four-stage system of restricting access to information with the classification of «Top Secret», «Top Secret», «Secret» and «Restricted». This system is provided for in the draft Law of Ukraine «On Security of Classified Information», taking into account the provisions of the National Security Strategy of Ukraine, NATO and European Union security standards. Its implementation allows for the creation of a new methodology for the effective functioning of the system of protection of classified information and improvement of the regulatory framework.*

Theoretical and practical significance of the article *for the military and defence sector. The improved methodology contributes to the development of information security theory by integrating NATO and EU international standards into the context of Ukraine's national defence, which allows for the creation of a unified*

security assessment system. It adapts approaches to assessing information security to modern threats and the specifics of the operational environment. The practical significance of the methodology lies in the ability to timely assess the level of information security, identify the causes of threats and develop measures to minimise the risks of information leakage or loss. Its implementation increases the efficiency of management of an operational grouping of troops (forces) in the area of hostilities.

Conclusion and the perspectives of future researches. *The developed system for protecting restricted information ensures reliable data transmission, operational coordination and decision-making in real time, which is crucial for the successful completion of combat missions. The direction of further research is to improve the model for assessing the damage to an operational grouping of troops (forces) in the event of a leak of classified information circulating in the subsystem of military command and control bodies, as well as to develop and implement relevant provisions in the legal acts regulating the organisation and security of information.*

Keywords: *information constituting a state secret, proprietary information, information security, operational grouping of troops (forces), importance factor, list of threats, security, information security system.*

References

1. On State Secrets [online], (1994). Zakon Ukrainy No. 3855-XII, 21 January. Available at: https://www.zakon.rada.gov.ua/ laws/show/3855–12 [Accessed 22 November 2024). **2. On Information** [online], (1992). Zakon Ukrainy No. 2657-XII, 02 October. Available at: https://www.zakon.rada.gov.ua/ laws/show/2657–12 [Accessed: 22 November 2024]. **3. Compendium of information constituting a state secret** [online], (2020). Order of the Security Service of Ukraine from 23 December No 383. Available at: https://www.zakon.rada.gov.ua/ laws/show/z0052–21 [Accessed: 22 November 2024]. **4. List of data of the Ministry of Defense of Ukraine containing proprietary information** [online], (2023). Ministry of Defence of Ukraine from 17 October No. 605. Available at: https://www.zakon.rada.gov.ua/rada/show/v0605322–23 [Accessed: 22 November 2024]. **5. National Security Strategy of Ukraine** [online], (2015). Decree of the President of Ukraine dated 26 May No. 287/2015. Available at: https://www.zakon.rada.gov.ua/laws/show/287 [Accessed: 22 November 2024]. **6. NATO Security Policy** (C-M(2002)49). Administrative Arrangements [online], (2017). Law of Ukraine dated May 24, No. 2068-VIII. Available at: https://www.uvns.hr/UserDocsImages/Nato%20-%20dokumenti/1%20C-M%282002%2949-REV1%20-%20Security%20Within%20the%20NATO.pdf [Accessed: 22 November 2024]. **7. EU Security Rules** 2013/488/EU / Council security rules for protecting classified information (EUCI) Council Decision of 23 september 2013 on the security rules for protecting EU classified information // URL: https://eur–lex.europa.eu/legal–content/EN/TXT/?uri=CELEX%3A32013D0488 [Accessed: 22 November 2024]. **8. On the Security of Classified Information** [online], (2023). Draft Law of the Verkhovna Rada of Ukraine No. 8394 dated January 27. Available at: https://www.itd.rada.gov.ua/billInfo/Bills/Card/41249 [Accessed: 22 November 2024]. **9. Vdovenko, S. G.,** (2015). Modern Requirements for the Protection of State Secrets and Protection of Restricted Information in a Special Period. *Imperatives of Civilization Development.* 2, 93-96. **10. Shkarlat, O. O., Shtonda, R. M., Sulimovska, M. V.,** (2018). Protection of information in automated systems of security entities. *Modern Information Technologies in the Sphere of Security and Defence.* 2 (32), 17-22. **11. Vdovenko, S. G., Gulak, J. S., Mashtalir, V. V.,** (2023). Legislative, regulatory and definitional aspects of the problems in the field of protection of state secrets and proprietary information in times of war and ways to solve them. *Actual Problems of Information Security of the State* : *proceedings of the XIV All-Ukrainian Scientific and Practical Conference, March 30,* Kyiv. **12. Shkarlat, O. O., Shtonda, R. M., Sulimovska, M. V.,** (2017). Protection of information in automated systems of security entities. *Modern Information Technologies in the Sphere of Security and Defence.* 2 (32). **13. Korchenko, O. H., Arhipov, O. E., Dreis, U.O.,** (2013). Assessment of Damage to Ukraine's National Security in the Event of a State Secret Leak : Monograph. NA of the SSU. Kyiv. **14. Standard Instruction** on the Procedure for Keeping Records, Storage, Use and Destruction of Documents and Other Material Media Containing Proprietary Information [online], (2016). Resolution of the Cabinet of Ministers from 19 October № 736. Available at: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text [Accessed: 22 November 2024].