МЕТОДИЧНИЙ ІНСТРУМЕНТАРІЙ ОЦІНЮВАННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНУ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

METHODOLOGICAL TOOLS FOR ASSESSING THE LEVEL OF INFORMATION SECURITY OF THE SECURITY SERVICE OF UKRAINE

УДК 351.74/.76
DOI https://doi.org/10.32843/2663-5240-2019-12-23

Харченко С.О.
здобувач кафедри національної безпеки (сфера прикордонної діяльності) та управління факультету підготовки керівних кадрів Національна академія Державної прикордонної служби України імені Богдана Хмельницького

У статті визначено, що інформаційна безпека є комплексом заходів та засобів щодо забезпечення збереження інформації, що знаходиться в системі інформаційного забезпечення діяльності органів Служби безпеки України. Запропоновано послідовність оцінювання рівня інформаційної безпеки органу Служби безпеки України, яка включає такі етапи: ідентифікація напрямів (груп) оцінювання та вибір показників; визначення алгоритму розрахунку показників оцінювання; стандартизація показників; розрахунок коефіцієнтів вагомості та верифікація їх значень; обчислення індексу інформаційної безпеки органу Служби безпеки України; ідентифікація рівня інформаційної безпеки та встановлення напрямів запобігання та нейтралізації інформаційних загроз. Для процедури оцінювання рівня інформаційної безпеки органу Служби безпеки України запропоновано використовувати три ключові напрями: оцінка програмно-технічної захищеності інформації (коефіцієнт технічного захисту інформації, коефіцієнт програмної захищеності інформації, коефіцієнт фінансового захисту інформації, коефіцієнт фінансування інформаційної служби); оцінка інформаційної надійності персоналу (коефіцієнт правової захищеності інформації, коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку установи, коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку, та коефіцієнт підготовленості персоналу до розпізнавання загроз); оцінка системи захисту інформації (ступінь інформаційного ризику; коефіцієнт реагування на зовнішні загрози інформаційній безпеці; коефіцієнт реагування на внутрішні загрози інформаційній безпеці; коефіцієнт керованості системи інформаційної безпеки установи). Індекс інформаційної безпеки органу Служби безпеки України розраховується на основі зважених на коефіцієнт вагомості групових індексів інформаційної безпеки. Отримане числове значення індексу порівнюється з встановленими нормативними інтервалами значень та дозволяє ідентифікувати високий, середній або низький рівень інформаційної безпеки органу служби безпеки України, що слугує основою розробки відповідних заходів щодо її збереження, стабілізації або підвищення.

Ключові слова: *інформаційна безпека органу Служби безпеки України, оцінка програмно-технічної захищеності інформації, оцінка інформаційної надійності персоналу, оцінка системи захисту інформації, індекс інформаційної безпеки органу Служби безпеки України.*

In the article it is stated that information security is a set of measures and means to ensure the security of the information whithin the system of information support for the activities of the bodies of the Security Services of Ukraine. The sequence of assessing the level of information security of the Security Service of Ukraine has been proposed. It includes the following steps: identification of areas (groups) of assessment and selection of indicators; determination of an algorithm for calculating assessment indicators; standardization of indicators; calculation of weighting coefficients and verification of their values; calculation of the information security index of a body of the Security Service of Ukraine; identification of the level of information security and the establishment of areas for preventing and neutralizing information threats. It is proposed to use three key areas for the procedure for assessing the level of information security of a body of the Security Service of Ukraine: assessment of software and hardware security of information (the coefficient of technical information security, the coefficient of software information security, the coefficient of financial information protection, the coefficient of financing the information service); assessment of information reliability of staff (the coefficient of legal information security, the coefficient of work experience of staff that ensure information security of an institution, the reliability coefficient of the staff providing information security and the coefficient of competence of the staff for recognizing threats); assessment of the information security system (the degree of information risk; the response coefficient to external threats to information security; the response coefficient to internal threats to information security; the controllability coefficient of information security system of an institution). The information security index of a body of the Security Service of Ukraine is calculated on the basis of grouped information security indices weighted by the weight coefficient. The obtained numerical value of the index is compared with the established normative ranges of values and allows identifying the high, medium or low level of information security of the bodies of the Security Service of Ukraine, and it serves as the basis for the development of appropriate measures for information security preservation, stabilization or increase.

Key words: *information security of a body of the Security Service of Ukraine, assessment of software and technical security of information, assessment of information reliability of personnel, assessment of the information security system, information security index of the bodies of the Security Service of Ukraine.*

Постановка проблеми у загальному вигляді. Однією з умов ефективної діяльності органів Служби безпеки України є використання ними можливостей інформаційного суспільства, яке створює єдиний глобальний інформаційний простір, що характеризується мінливою та високою інтенсивністю інформаційних процесів. На сучасному етапі розвитку України як економічно розвиненої та правової держави особливе місце займає національна безпека, важливим складником якої є інформаційна. Держава, яка має розвинені інфор-

маційні системи та засоби інформаційного захисту, є лідером в економічній, політичній та соціальній сферах, має стратегічну і тактичну переваги, зокрема у передових інформаційних технологіях.

В останні роки суспільні відносини в Україні розвиваються у пришвидшеному темпі. Не завжди як наукова спільнота, так і законодавство встигають осмислити та упорядкувати відповідними правовими способами наявний стан суспільних відносин. Вищезгадане зумовлює необхідність розробки нових критеріїв формування інформаційної безпеки органів Служби безпеки України, створення дієвих механізмів її регулювання, удосконалення й приведення вітчизняної практики у відповідність до міжнародних стандартів. Недостатня наукова опрацьованість вказаної проблематики науковцями не сприяє виробленню ефективного підходу до упорядкування відповідних суспільних відносин.

Аналіз останніх досліджень і публікацій. Основне теоретичне підґрунтя дослідження у сфері інформаційної безпеки становлять праці таких відомих вчених, як В.А. Ліпкан, Ю.Є. Максименко, О.В. Олійник, І.М. Олійченко, О.С. Онищенко, В.М. Петрик, С.М. Попова, Г.П. Ситник, А.В. Шапка, О.К. Юдін, В.І. Ярочкин та інших.

Виділення невирішених раніше частин загальної проблеми. Віддаючи належне результатам, отриманим зазначеними та іншими вченими, слід наголосити, що теоретичні та науково-практичні засади, напрями та механізми забезпечення інформаційної безпеки органів Служби безпеки України залишаються недостатньо обґрунтованими. Зокрема, додаткового опрацювання потребує методичний інструментарій оцінювання рівня інформаційної безпеки органів СБУ. Зазначені обставини зумовлюють актуальність та науково-практичну значущість пропонованої статті.

Мета статті. Враховуючи вищезазначене, метою цієї статті є опрацювання методичного інструментарію оцінювання рівня інформаційної безпеки органів СБУ як основи розробки системи заходів підвищення інформаційної захищеності функціонування силових структур.

Виклад основного матеріалу дослідження. Інформаційна безпека є комплексом заходів та засобів щодо забезпечення збереження інформації, що знаходиться в системі інформаційного забезпечення діяльності органу Служби безпеки України. Призначення системи інформаційної безпеки органів Служби безпеки України полягає в організації безпечних і надійних заходів з доступу до інформації, способів передачі та зберігання інформації, методів обробки інформації, правил управління доступом до інформації, що становить державну таємницю або є інформацією для службового користування, способів відновлення інформації, методів резервування інформації тощо.

Оцінювання рівня інформаційної безпеки органів Служби безпеки України пропонуємо проводити за трьома ключовими напрямами: оцінка програмно-технічної захищеності інформації; оцінка інформаційної надійності персоналу; оцінка системи захисту інформації [1].

Своєю чергою оцінку програмно-технічної захищеності інформації доцільно проводити за такими показниками: коефіцієнт технічного захисту інформації, коефіцієнт програмної захищеності інформації, коефіцієнт фінансового захисту інформації, коефіцієнт фінансування інформаційної служби.

Для оцінки інформаційної надійності персоналу органів Служби безпеки України пропонуємо розраховувати коефіцієнт правової захищеності інформації, коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку установи, коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку, та коефіцієнт підготовленості персоналу до розпізнавання загроз [2; 3; 4].

Оцінку системи захисту інформації пропонуємо проводити за допомогою таких показників: ступінь інформаційного ризику; коефіцієнт реагування на зовнішні загрози інформаційній безпеці; коефіцієнт реагування на внутрішні загрози інформаційній безпеці; коефіцієнт керованості системи інформаційної безпеки установи. Варто зазначити, що для отримання інформації, необхідної для розрахунку наведених показників, обов'язковою умовою є наявність системи моніторингу діяльності органів Служби безпеки України [5, с. 76]. Система показників оцінки рівня інформаційної безпеки органу Служби безпеки України за кожним з запропонованих напрямів з розрахунковими формулами та граничними значеннями наведена в табл. 1.

Запропоновані нами показники оцінки рівня інформаційної безпеки органів Служби безпеки України мають різну розмірність і не можуть бути агреговані в інтегральний коефіцієнт, тому необхідним є застосування процедури нормування (уніфікації) і переведення дестимуляторів в стимулятори. Оскільки в процесі розрахунку ми використовуємо як показники-стимулятори, зростання яких є бажаним для рівня інформаційної безпеки, так і дестимулятори, зростання яких негативно відображається на інформаційній

Таблиця 1

Система показників оцінки рівня інформаційної безпеки органу Служби безпеки України

№ з/п	Назва показника	Алгоритм розрахунку	Еталонне значення	Характеристика впливу на кінцевий показник
1.	Оцінка програмно-технічної захищеності інформації			
1.1	Коефіцієнт технічного захисту інформації Кт.з.	Кт.з. = ІАн.В., де ІАн.в. – кількість не відвернутих інформаційних атак.	0	дестимулятор
1.2	Коефіцієнт програмної захищеності інформації Кп.з.	Кп.з. = Чб.ф./ Чб.ф., де Чб.ф. – час безперебійного функціонування інформаційної системи, год.; Чн.ф. – нормативний час функціонування інформаційної системи, год.	1	стимулятор
1.3	Коефіцієнт фінансового захисту інформації Кф.з.	Кф.з. = Вз.ін. / Впр.ін., де Вз.ін. – витрати на захист інформаційних ресурсів, грн.; Впр.ін. – витрати на придбання інформаційних ресурсів, грн.	0,1	дестимулятор
1.4	Коефіцієнт фінансування інформаційної служби Кфін.	Кфін. = Кфін./Вз, де Вфін. – витрати на фінансування інформаційної служби установи, грн.; Вз – загальні витрати установи.	0,05	дестимулятор
2.	Оцінка інформаційної надійності персоналу			
2.1	Коефіцієнт правової захищеності інформації Кпр.з.	Кпр.з.= І/Іюр.з, де І – обсяг інформації, розголошення якої може спричинити негативні наслідки для установи, %; Іюр.з. – загальний обсяг юридично захищеної інформації, %.	0,2, зменшення	дестимулятор
2.2	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку Кд.р.	Кд.р. = ЧПін/ ЧПз, де ЧПін – чисельність працівників, які мають доступ до інформації для службового використання, що працюють в установі більше одного року, ос.; ЧПз – загальна чисельність працівників, що мають доступ до інформації для службового використання, ос.	1	стимулятор
2.3	Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку Кн.п.	Кн.п. = (ЧПз.зв – ЧПвін)/ ЧПз.зв, де ЧПвін – чисельність працівників, звільнених за причиною витоку інформації, осіб; ЧПз.зв. – загальна чисельність звільнених працівників, осіб.	1	стимулятор
2.4	Коефіцієнт підготовленості персоналу до розпізнавання погроз Кпп	Кпп = (ЧПз- ЧПп)/ ЧПз де ЧПп – чисельність працівників, ненавмисні дії яких призвели до витоку інформації завдяки низькому рівню підготовки персоналу до розпізнавання загроз безпеки, осіб; ЧПз – загальна чисельність працівників, що мають доступ до інформації для службового використання, осіб.	1	стимулятор
3.	Оцінка системи захисту інформації			
3.1	Ступінь інформаційного ризику (Ір)	Ір= Інз/Інб., де Інз – кількість невідвернутих інформаційних загроз, од.; Інб.– загальна кількість загроз інформаційній безпеці, од.	0	дестимулятор
3.2	Коефіцієнт реагування на зовнішні загрози інформаційній безпеці (Крзз)	Крзз= Квзз/ Кзз, де Квзз – кількість відвернутих зовнішніх загроз інформаційній безпеці, од.; Кзз – загальна кількість зовнішніх загроз інформаційній безпеці, од.	1	стимулятор
3.3	Коефіцієнт реагування на внутрішні загрози інформаційній безпеці (Крвз)	Крвз= Кввз/ Квз де Кввз – кількість відвернутих внутрішніх загроз інформаційній безпеці, од.; Квз – загальна кількість внутрішніх загроз інформаційній безпеці, од.	1	стимулятор
3.4	Коефіцієнт керованості системи інформаційної безпеки установи (Ккс)	Ккс= Кф/Кфн., де Кф – кількість функцій, які виконуються в межах установи по забезпеченню інформаційної безпеки, од.; Кфн – загальна кількість функцій, що має виконуватись в установі по забезпеченню інформаційної безпеки, згідно з інструктивними документами, од.	1	стимулятор

Примітка: складено автором

захищеності установи, то під час розрахунку будемо застосовувати стандартний підхід, який репрезентований інструментарієм математичної статистики. Так, для стандартизації показників будемо використовувати такі формули:

а) для стимуляторів:

$$\overline{x}_{ij} = x_{ijp}, \quad (1)$$

б) для дестимуляторів:

$$\overline{x}_{ij} = 1 - x_{ijp}, \quad (2)$$

де $\overline{E}_{ij}$ – нормоване значення і-того показника в j-тій групі; хijp – розрахункове значення і-того показника в j-тій групі.

Наступною процедурою оцінювання рівня інформаційної безпеки органу Служби безпеки України є встановлення вагових коефіцієнтів оціночних показників. Це зумовлено різним рівнем впливу показників на розвиток та динаміку відповідного явища. З цією метою використовують різні підходи, такі як метод упорядкування рангів та експертне оцінювання. На практиці найбільш вживаним є експертний метод встановлення вагових значень показників, що зумовлено відносною простотою його застосування. Однак цьому методу притаманний високий рівень суб'єктивізму та трудомісткість збору результатів.

Щоб забезпечити коректність оцінювання, ми запропонували десятьом експертам (фахівцям у галузі інформаційної безпеки) визначити ступінь значимості показників, тобто встановити ступінь їх впливу на забезпечення економічної безпеки регіону. Експерти проранжували всі показники за ступенем важливості за шкалою від 1 до 10 балів (10 – здійснює найбільший вплив; 1 – вплив цього показника найменший). У результаті вагомість кожного показника ми розрахували за формулою:

$$K_{ві} = \frac{\sum_{k=0}^{10} Б_{ijk}}{\sum_{k=0}^{10} Б_{jk}}, \quad (3)$$

де $K_{ві}$ – коефіцієнт вагомості i-го показника; d – номер експерта; K – кількість експертів в групі; $Б_{ijk}$ – бал, привласнений i-му показнику j-тої групи k-м експертом; $Б_{jk}$ – сума балів, привласнених k-м експертом всім показникам j-тої групи.

Під час проведення розрахунків сума вагомості всіх показників певної групи буде дорівнювати 1. Отримані нами в процесі обчислень коефіцієнти вагомості представлено в табл. 2.

Наступний етап передбачає визначення проміжних та загального індексу рівня інформаційної безпеки органів Служби безпеки України. Спочатку необхідно розрахувати групові індекси. Для цього пропонуємо використовувати формулу 4.

Таблиця 2

Вагові коефіцієнти показників оцінки рівня інформаційної безпеки

№ з/п	Назва показника	Вагові коефіцієнти
1.	Оцінка програмно-технічної захищеності інформації	0,3892
1.1	Коефіцієнт технічного захисту інформації (Кт.з.)	0,2852
1.2	Коефіцієнт програмної захищеності інформації (Кп.з.)	0,2879
1.3	Коефіцієнт фінансового захисту інформації (Кф.з.)	0,2478
1.4	Коефіцієнт фінансування інформаційної служби (Кфін.)	0,1791
2.	Оцінка інформаційної надійності персоналу	0,3147
2.1	Коефіцієнт правової захищеності інформації (Кпр.з.)	0,1472
2.2	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку (Кд.р.)	0,2157
2.3	Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку (Кн.п.)	0,3245
2.4	Коефіцієнт підготовленості персоналу до розпізнавання погроз (Кпп)	0,3126
3.	Оцінка системи захисту інформації	0,2961
3.1	Ступінь інформаційного ризику (Ір)	0,2468
3.2	Коефіцієнт реагування на зовнішні загрози інформаційній безпеці (Крзз)	0,2165
3.3	Коефіцієнт реагування на внутрішні загрози інформаційній безпеці (Крвз)	0,2682
3.4	Коефіцієнт керованості системи інформаційної безпеки установи (Ккс)	0,2685

Примітка: розраховано автором

$$I_{гр_j} = \sum_{i=1}^{n} K_{ві} \cdot \overline{x}_{ij}, \quad (4)$$

де $I_{гpj}$ – груповий індекс інформаційної безпеки показників j-тої групи; $\overline{x}_{ij5}$ – нормоване значення і-го показника інформаційної безпеки j-тої групи; $K_{ві}$ – коефіцієнт вагомості i-го показника.

Обчислення інтегрального коефіцієнта інформаційної безпеки органу Служби безпеки України пропонуємо проводити із використанням формули 5:

$$I_{ІБ} = \sum_{j=1}^{3} K_{вj} \cdot I_{гpj}, \quad (5)$$

де $I_{ІБ}$ – інтегральний індекс інформаційної безпеки органу Служби безпеки України; $K_{вj}$ – коефіцієнт вагомості j-тої групи показників.

Наступний крок передбачає інтерпретацію результатів оцінки та порівняння отриманого індексу інформаційної безпеки з встановленими інтервальними значеннями. Під час визначення рівня інформаційної безпеки органу Служби безпеки України важливим є визначення ключових точок, досягнення яких означатиме певний рівень розвитку. Опрацьована модель індексу (формула 5) передбачає, що за I_{ippj} = 0 рівень інформаційної безпеки органу Служби безпеки України значно нижчий за середній по сукупності, а за I_{ippj} =1, навпаки, значно вищий. Для більш ґрунтовної інтерпретації отриманих результатів пропонуємо шляхом інтервального розподілу значень індексу виділяти три рівні інформаційної безпеки органу Служби безпеки України: низький, середній та високий (табл. 3).

Таблиця 3

Ідентифікація рівня інформаційної безпеки органу СБУ відповідно до розміру інтервалу

Інтервальні значення індексу інформаційної безпеки органу СБУ	(0–0,33)	(0,34–0,66)	(0,67–1)
Інтерпретація значень показника	Низький рівень	Середній рівень	Високий рівень

Примітка: розроблено автором

Отримані числові значення індексу дозволяють провести рейтингування органів Служби безпеки України за рівнем інформаційної безпеки від найменшого числового значення (найближчого до 0) до найвищого (такого, що наближається до 1). На основі отриманих числових значень індексу можна здійснити розробку комплексу заходів зміцнення інформаційної безпеки органу Служби безпеки України, а глибинний аналіз розрахованих коефіцієнтів дасть можливість визначити «критичні точки», вплив на які забезпечить підвищення рівня захисту інформації в установі.

Висновки. Таким чином, використання пропонованого підходу до оцінювання рівня інформаційної безпеки органу Служби безпеки України дозволить не лише ідентифікувати рівень інформаційної захищеності установи, але й визначити напрями підвищення ефективності використання інформаційних ресурсів та збалансувати витрати на забезпечення інформаційної безпеки. Подальші дослідження можливі в контексті доповнення або перегляду сукупності показників оцінювання та розробки комплексу заходів для підвищення рівня інформаційної безпеки органу Служби безпеки України.

ЛІТЕРАТУРА:

1. ISO/TC 176/SC 2/N 544R2, ISO 9000: Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems. 13 May 2004

2. Technical Report ISO/IEC TR 18044. Information technology – Security techniques – *Information security incident management.*

3. Deming W. Edward. Out of the Crisis: Quality, Productivity, and Competitive Position. Mass. Inst. of Technology, Center for Advanced Engineering Study: Cambridge University Press, Cambridge (Mass.) 1982.

4. NIST Special Publication 800-61, Computer Security Incident Handling Guide. *Recommendations of the National Institute of Standards and Technology.* January 2004.

5. Курило А.П. Аудит информационной безопасности. [Текст] / Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. Москва : Издательская группа «БДЦ-пресс», 2006. 420 с.