УДК 681.3.06

ПІДХІД ДО ЗДІЙСНЕННЯ КОНТРОЛЮ ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗГІДНО ISO/IEC 27001 НА ОСНОВІ ОБРОБКИ МЕТРИЧНИХ ПОКАЗНИКІВ БЕЗПЕКИ МЕТОДАМИ СИСТЕМНОГО АНАЛІЗУ

А.В. ЛЄНШИН, М.А. ВЕЛИЧКО

Розглядаються сучасні системи метричних показників безпеки. Розробляється сукупність показників для оцінювання ступеня впровадження системи управління інформаційною безпекою. Наводяться формальні постановки задач оцінювання відповідності поточних та цільових значень метричних показників безпеки. Розглядаються приклади розв'язання сформульованих задач контролю.

Ключові слова: система управління інформаційною безпекою, ISO/IEC 27001, метричні показники безпеки, системний аналіз.

ВСТУП

Прийнятий у 2005 році міжнародний стандарт ISO/IEC 27001 [1] визначає модель створення, впровадження, експлуатації, постійного контролю, аналізу, підтримки в робочому стані та вдосконалення системи управління інформаційною безпекою (СУІБ). Оскільки діяльність із захисту інформації, пов'язана в першу чергу саме з управлінням інформаційною безпекою – стандарт ISO/IEC 27001 де-факто вважається одним з базових стандартів галузі. Актуальність дослідження процесів впровадження ISO/IEC 27001 зумовлюється його фундаментальним значенням для теорії та практики захисту інформації, а також нещодавнім прийняттям його в якості галузевого стандарту Нацбанку України.

Ідеологія стандарту полягає не стільки в висуванні конкретних вимог до СУІБ, скільки в постійному покращені якості їх виконання. Така особливість пов'язана з вимогою "універсальності", тобто застосовності положень стандарту до організацій будь-якого типу та розміру, а також наявності обмежень (зокрема, фінансових), що існують в організації. ISO/IEC 27001 пропонує підхід до побудови СУІБ згідно моделі PDCA (Plan-Do-Check-Act), що дає змогу сертифікувати організацію не за зразкове та бездоганно-повне виконання вимог стандарту, а за поступове та безперервне вдосконалення СУІБ з метою досягнення визначеного рівня за визначений проміжок часу.

Отже розв'язання задач контролю ефективності заходів, що здійснюються організацією для впровадження/супроводу СУІБ, є необхідною її передумовою її впровадження. Очевидно, що процедура контролю має засновуватись не лише з використанням експертних оцінок, але і на аналітичних даних, що відображатимуть рівень планомірності здійснення заходів та відповідність реального та цільового обсягу виконаних заходів. Для отримання таких даних пропонується розробити систему показників безпеки, яка дасть змогу зібрати необхідну інформацію та обробити її. Під обробкою розуміється перетворення, результатом якого є кількісне або якісне значення, що відображає поточну відповідність організації вимогам розділів 4, 5, 6, 7, 8 та Додатку А стандарту ISO/IEC 27001. На роль такої системи показників можуть претендувати системи метричних показників безпеки. Найбільш відомими системами такого класу є: Vaugh-Hennig–Siraj, NIST, OCIPEP, OCTAVE, CISWG та система показників Erkan Kahrman [2]. Зазначені системи можна класифікувати за змістом їх метричних показників та розділити на системи з кількісними (система CISWG), якісними (система OCTAVE) та змішаними показниками (система NIST, Erkan Kahrman). Серед них слід виділити систему NIST та систему Kahrman як системи, що охоплюють найбільш широкий спектр аспектів інформаційної безпеки.

1. РОЗРОБКА СИСТЕМИ МЕТРИЧНИХ ПОКАЗНИКІВ БЕЗПЕКИ ДЛЯ ISO/IEC 27001

Прийнятий зусиллями підкомітету SC27 "Методи захисту IT", зі складу спільного технічного комітету ISO/IEC JTC1, "Інформаційні технології", стандарт ISO/IEC 27004 [3] пропонує методику створення метричних показників, а саме рекомендації з розробки показника, загальну модель показника та приклади для кожної з областей вимірювань (табл. 1). Поточна версія стандарту визначає 10 областей вимірювань та мінімум по одному прикладу показника до кожної з них.

Виходячи з таблиці 1, систему показників згідно з ISO/IEC 27004 можна класифікувати як систему зі змішаними показниками. Проте ISO/IEC 27004 не надає жодних пропозицій щодо процедури об'єднання значень показників з метою подальшого представлення значення групи показників, і отже питання об'єднання кількісних показників з кількісними, якісних з якісними та кількісні з якісними є невирішеним так саме, як і питання інтерпретації отриманих результатів об'єднання. Система показників охоплює не лише Додаток А, а й пункти 4, 5, 6, 7, 8 вимог ISO/IEC 27001.

Враховуючи те, що жодна з існуючих систем показників безпеки не може охопити множину вимог ISO/IEC 27001 в повному обсязі, а ISO/IEC 27004, присвячений вимірюванням в сфері інформаційної безпеки, пропонує лише приклади показників – задача практичної розробки

Таблиця 1

Показники безпеки згідно з ISO/IEC 27004, що визначені для ISO/IEC 27001

Назва показника	Призначення виміру	Показник	Можливе значення показника
СУІБ – свідомість персоналу	Пункт 5.2.2.d	Доля співробітників, що пройшли навчання СУІБ	0-100%
Політики паролів	Пункт 11.3.1 Додатку А	Доля паролів, що задовольняють вимогам політики паролів організації	0-1
Постійне та безперервне вдосконалення СУІБ	Пункт 4.2.2 h	Вдосконалення СУІБ обчислюється як кількість інцидентів інформаційної безпеки за проміжок часу	Незадовільно, задовільно, добре
Антивірусний захист	Пункт 10.4.1 Додатку А	Кількість інцидентів, що спричинені вірусними програмами. Тенденція	Поліпшення, погіршення, значне погіршення
Проведення періодичного обслуговування	Пункт 9.2 Додатку А	Тривалість затримки, що мала місце на момент обслуговування	Не визначено
Перегляд журналу подій	Пункт 10.10.2 Додатку А	Відсоток контрольних файлів журналу, переглянутих на встановлений момент часу	0-100%

системи показників безпеки безпосередньо для ISO/IEC 27001 є доцільною та обґрунтованою. Цю задачу пропонується розв'язувати на основі врахування вимог та рекомендацій ISO/IEC 27004, NIST SP 800-53 та NIST SP 800-55 [4]. Модель показника згідно з NIST SP 800-55 та ISO/IEC 27004, а також детальний опис розробленого за нею метричного показника представлена в табл. 2. У табл. 3 наведені стислий опис показників, що були розроблені для пункту А.5.1 стандарту ISO/IEC 27001. Розроблену авторами систему показників слід віднести до змішаного типу через те, що вона має кількісні та якісні показники, чим зумовлюється необхідність їх узагальнення і отримання комплексної оцінки: загальної та в межах області. Система налічує показники трьох типів: контрольний лист (так/ні), розрахунок за формулою та аналіз (вибір однієї з множини запропонованих відповідей).

Узагальнення показників пропонується здійснювати шляхом введення єдиної шкали та зведення до неї всіх типів показників. А саме: для підвищення точності результатів та відсутності дробових значень шкала має розмірність 100. Тип «контрольний лист» має значення 100 або 0 в залежності від варіанту відповіді. Тип «розрахунок» приймає значення від 0 до 100 в залежності від розрахованого у відсотках значення. Третій тип «аналіз», у випадку

Таблиця 2

Модель та приклад розробленого показника безпеки згідно з NIST SP 800-55

Визначено у NIST		Приклад розробленого показника
Поле	Дані	Дані
ID показника	Унікальний ідентифікатор показника	SP-1.2
Мета	Вказується стратегічна мета впровадження та/або мета з точки зору інформаційної безпеки	Стратегічна мета: забезпечення належного середовища функціонування СУІБ. Мета з точки зору інформаційної безпеки: забезпечення правил політики безпеки
Вимір	Відсотки, кількість, частота, середня величина	Відсотки. Доля співробітників, що ознайомлені з політикою безпеки. NIST SP 800-53 Control: AC-1: Access Control Policy and Procedures
Профіль	Що визначає. Ефективність, виконання чи вплив	Ефективність
Формула розрахунку	Представляється формула, за якою обчислюється результат	(Кількість співробітників, що ознайомлені з політикою безпеки)/(загальна кількість співробітників)
Необхідне значення	Вказується поріг значення, при якому воно вважається задовільним	Визначається організацією
Реалізація	Опис безпосередньо показника. Вказується контрольне питання з варіантами відповідей або параметрами	Скільки співробітників ознайомлено з політикою безпеки? Яка загальна кількість співробітників?
Регулярність застосування	Вказується регулярність збору даних, їх аналізу та частота звертання	Визначається організацією
Відповідальні сторони	Вказується відповідальні сторони, а саме: власник, відповідальний за збір інформації та замовник	Власник: визначається організацією Відповідальний за збір інформації: визначається організацією Замовник: визначається організацією
Джерело даних	Вказується джерело даних	Визначається організацією
Формат звітності	Описується формат представлення результатів	Кругова діаграма. Відсоток ознайомлених з політикою співробітників

Таблиця 3

Приклади розроблених показників для пункту А.5.1 з ISO/IEC 27001

Політика захисту інформації				
SP-1.1	Пункт 5.1.1 Додатку А	Чи має організація опубліковану політику безпеки, затверджену керівництвом?	Так/Ні	0, 100
SP-1.2	Пункт 5.1.1 Додатку А	Яку частину співробітників та ознайомлено з політикою безпеки?	Відношення кількості співробітників, що ознайомлені з політикою безпеки до загальної кількості. Відсоток.	0-100
SP-1.3	Пункт 5.1.1 Додатку А	Який відсоток відділів має останню версію політики безпеки?	Обчислюється як відношення кількості відділів, що мають останню редакцію до загальної кількості відділів. Відсоток.	0-100
SP-2.1	Пункт 5.1.2 Додатку А	Чи заплановано інтервали для оновлення політики безпеки?	Так/Ні	0, 100
SP-2.2	Пункт 5.1.2 Додатку А	Який інтервал часу заплановано для оновлення політики безпеки?	Вибір варіанту відповіді: раз на місяць; раз в 2 місяці; щоквартально; раз в півроку; раз на рік.	100, 75, 50, 25, 0
SP-2.3	Пункт 5.1.2 Додатку А	Оновлення політика в разі серйозних змін?	Обчислюється як відношення кількості оновлень політики внаслідок змін системи до загальної кількості серйозних змін системи. Відсоток.	0-100

п'яти варіантів відповідей, приймає значення 0, 25, 50, 75, 100 балів відповідно.

2. ФОРМАЛЬНІ ПОСТАНОВКИ ЗАДАЧ КОНТРОЛЮ ВПРОВАДЖЕННЯ СУІБ

Використання розробленої системою метричних показників безпеки дозволяє отримати значення в балах, знаючи максимально можливу кількість балів результат можна звести до відсотків. Наприклад, якщо в результаті обчислень за допомогою системи метричних показників отримали значення 76% та 80% відповідності стандарту на двох проміжках часу, може виникнути питання як саме інтерпретувати ці значення, які висновки можна зробити та як подібні значення відображають покращення СУІБ у часі? Очевидно, що у такому (та подібних) випадку корисною є використання відповідної методики розрахунку.

Для отримання якісної оцінки пропонується підхід, що є вдосконаленням підходів до контролю впровадження СУІБ. Підхід є розвитком методу, що був запропонований для оцінювання відповідності поточної та цільової зрілості процесів захисту інформації у роботі[5].

Застосування підходу передбачає наявність початкового значення відповідності (ПчЗВ), поточного значення відповідності (ПЗВ), введення цільового значення відповідності (ЦЗВ) вимогам стандарту та проміжного значення відповідності (ПрЗВ) в деяких контрольних точках. Такий підхід може застосовуватись лише за наступних умов: визначено час початку робіт, а також час, в який має бути досягнуте цільове значення відповідності.

Сутність методу отримання якісної оцінки зводиться до отримання значень планомірності впроваджених заходів, порівняння відповідності поточного значення відповідності з цільовим значенням та визначення відповідності цільового та реального обсягів виконаних заходів із вдосконалення СУІБ. Ступінь досягнення результату зручно представляти у вигляді радіальної діаграми (рис. 1). Діаграма демонструє поточне значення відповідності для 8 областей вимірювання та необхідний результат, що має бути досягнуто. Подібним чином представляються результати сертифікації за стандартом СТО БР ІББС-1.2-2010.

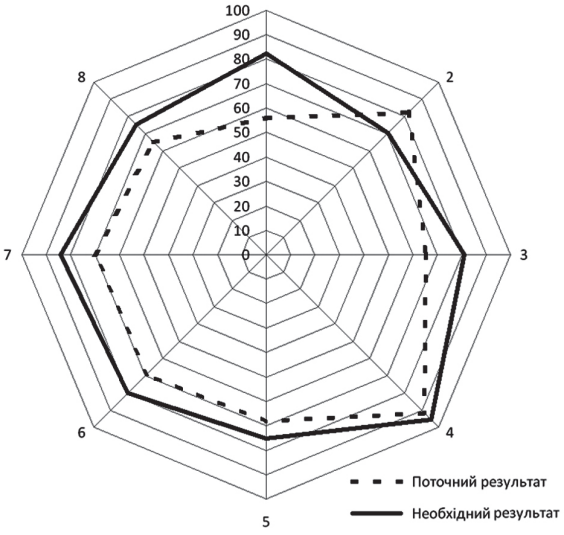

Рис. 1. Ступінь досягнення результату в момент часу t_i

Наведемо (застосовуючи прийняті скорочення та припущення) формальні постановки задач, що мають вирішуватися у ході контролю впровадження ISO/IEC 27001.

Задача 1. Перевірка поточної відповідності вимогам цільовим орієнтирам у контрольних точках.

Нехай для організації визначено поточне значення відповідності вимогам $\text{ПЗВ}(t_i)$ в момент часу t_i. Тоді за умови, що для t_i відоме значення проміжного значення відповідності вимогам $\text{ПрЗВ}(t_i)$, значенням показника поточної відповідності вимогам цільовим орієнтирам є значення $W(\text{ПрЗВ}(t_i), \text{ПЗВ}(t_i))$.

Якщо значення $\text{ПрЗВ}(t_i)$ для моменту t_i невідоме, то воно обчислюється на основі знання $\text{ПЗВ}(t_i)$ та ЦЗВ виходячи з припущення, що заходи щодо підвищення поточної відповідності

вимогам ПЗВ здійснюються рівномірно на інтервалі часу $(t_0;t_K)$ за виразом (1).

$$\text{ПрЗВ}(t_i)'' = \left\{\text{прзв}(t_i)_j''\right\}, j=\overline{1,n},$$

$$\text{прзв}(t_i)_j'' = \text{пзв}(t_0)_j + kt\cdot\left(\text{цзв}_j - \text{пзв}(t_0)_j\right), \quad (1)$$

де коефіцієнт kt розраховується за формулою (2) та дорівнює частині часу, що виділений на підвищення відповідності вимогам ПЗВ, яка минула на момент часу t_i:

$$kt = \frac{t_i - t_0}{t_K - t_0}. \quad (2)$$

Сутністю задачі 2 на відміну від задачі 1 є не обчислення відповідності абсолютних значень ПЗВ заданим цільовим орієнтирам, а з'ясування факту планомірності здійснення заходів з підвищення відповідності. Під планомірністю розуміється пропорційність досягнутих результатів результатам, що мають бути досягнуті в момент часу t_i згідно вимог ЦЗВ.

Задача 2. Перевірка планомірності здійснення заходів з впровадження СУІБ.

Нехай для організації визначено поточне значення відповідності вимогам ПЗВ в момент часу t_i та відоме значення проміжного цільового значення ПрЗВ (t_i), тоді значенням показника планомірності буде $W\left(\Delta\text{ПрЗВ}_{(t_i)}, \Delta\text{ПЗВ}_{(t_0,t_i)}\right)$.

Задача 3. Порівняння діяльності з впровадження СУІБ в кількох підрозділах або філіях організації.

Нехай існує організація, що складається з двох підрозділів A та B, для кожного з яких окремо визначено проміжні цільові значення відповідності вимогам ($\text{ПрЗВ}\ (t_i)$, $\text{ПрЗВ}^B(t_i)$) та визначено поточні значення відповідності вимогам ($\text{ПЗВ}\ (t_i)$, $\text{ПЗВ}^B(t_i)$) у контрольній точці t_i. Тоді задача порівняння зводиться до вирішення задачі 1 для кожного з підрозділів, тобто до обчислення $W\left(\text{ПрЗВ}^A(t_i), \text{ПЗВ}^A(t_i)\right)$ та $W\left(\text{ПрЗВ}^B(t_i), \text{ПЗВ}^B(t_i)\right)$ з наступним порівнянням отриманих значень включення. Підрозділ, в якому значення W більше, вважається таким, в якому діяльність з впровадження СУІБ здійснюється на більш високому рівні.

Задача 4. Визначення відповідності цільового та реального обсягу виконаних заходів з впровадження СУІБ.

Нехай існує організація, в якій здійснюються роботи з впровадження СУІБ згідно з дельта-проміжними цільовими значеннями відповідності $\Delta\text{ПрЗВ}_{(t_i)}$. Тоді на основі дельта-поточного значення відповідності $\Delta\text{ПЗВ}_{(t_0,t_i)}$ в контрольній точці t_i можна провести перевірку відповідності цільового та реального обсягу виконаних заходів з підвищення відповідності вимогам, за рахунок обчислення коефіцієнту φ, $0\le\varphi\le N$, де N – розмірність шкали оцінки рівня відповідності.

$$\varphi = \frac{\#\left(\Delta\text{ПЗВ}_{(t_0,t_i)}\right)}{\#\left(\Delta\text{ПрЗВ}_{(t_i)}\right)}. \quad (3)$$

Якщо значення φ дорівнює одиниці – реальні обсяги дорівнюють запланованим, якщо менше одиниці – відстають від них, значення більше одиниці – вказує на перевиконання плану в кількісному сенсі.

Вирішення сформульованих задач складається з приймання рішень відносно ступеню задоволення вимог одного набору значень відповідності іншим (включення), що відбиває різну ступінь включення одного об'єкта в інший та дозволяє виявити, який з об'єктів містить більше специфічних властивостей. Мірою включення значення відповідності є невід'ємна дійсна функція $W\left(\text{ЗВ}_i, \text{ЗВ}_j\right)$, що має такі властивості (4):

$$0\le W\left(\text{ЗВ}_i, \text{ЗВ}_j\right)\le 1 \text{ для } i\ne j;$$
$$W\left(\text{ЗВ}_i, \text{ЗВ}_j\right)=1 \text{ для } i=j. \quad (4)$$

Міра включення є несиметричною, отже включення ЗВ_i в ЗВ_j визначається як:

$$W\left(\text{ЗВ}_i, \text{ЗВ}_j\right) = \frac{\#\left(\text{ЗВ}_i \cap \text{ЗВ}_j\right)}{\#\left(\text{ЗВ}_i\right)}. \quad (5)$$

Загальне значення відповідності ЗВ_i описуються множиною оцінок поточних значень відповідності ПЗВ. Оскільки значення мають дискретні або дійсні значення, то для розрахунку значення міри включення необхідно використовувати поняття дескриптивної множини та визначити міри перетинання, об'єднання двох множин згідно таких виразів:

$$\#\left(\text{ЗВ}_i \cap \text{ЗВ}_j\right) = \sum_{r=1}^{q}\min\left(ml_{ri}, ml_{rj}\right)$$
$$\#\left(\text{ЗВ}_i \cup \text{ЗВ}_j\right) = \sum_{r=1}^{q}\max\left(ml_{ri}, ml_{rj}\right), \quad (6)$$

де ml – поточне значення відповідності вимогам ПЗВ, q – кількість ознак, що входять до загального значення відповідності. В результаті отримаємо значення включення у відсотках.

Наступним етапом є введення лінгвістичної змінної L = «Ступінь близькості», що може приймати значення L = {Дуже низька ступінь, Низька ступінь, Середня ступінь, Висока ступінь, Дуже висока ступінь відповідності} та проекція її на деяку шкалу з симетричним розташуванням вузлів класифікації (в точках 0.1, 0.5, 0.7, 0.9).

В якості шкали обрано так звану «сіру» шкалу Поспєлова, що являє собою полярну (опозиційну) шкалу, в якій перехід від властивості А+ до властивості А–. Шкала відображає зростання (спадання) непевності експерта $\mu(x)$ в класифікації з віддаленням від вузла. В результаті з'являється можливість звести числові значення до якісної форми представлення (рис. 2).

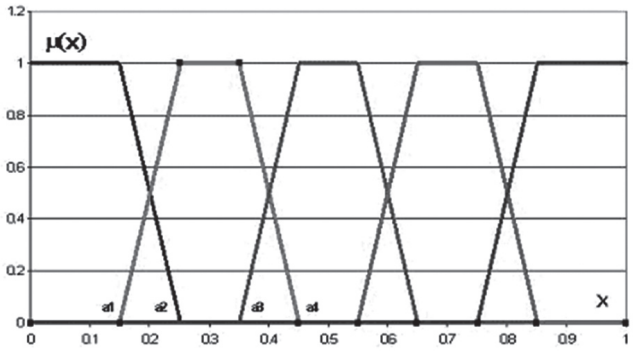

Рис. 2. Родина функцій належності змінної L на носій класифікації

3. ПРИКЛАДИ РОЗВ'ЯЗАННЯ ЗАДАЧ КОНТРОЛЮ ВПРОВАДЖЕННЯ СУІБ

Розглянемо приклади розв'язання задачі перевірки планомірності впровадження заходів з підвищення ефективності системи управління інформаційною безпекою.

Приклад 1. Постановка задачі.

Нехай для організації визначено поточне значення відповідності $\text{ПЗВ}(t_i)$ для n метричних показників безпеки ($AR_a, a=\overline{1,n}$), що характеризують ступінь впровадження заходів певної області вимог стандарту ISO/IEC 27001 в момент часу t_i та відоме значення проміжного значення відповідності $\text{ПрЗВ}(t_i)$. Необхідно перевірити планомірність здійснення заходів з підвищення ефективності СУІБ, за умови, що відоме значення початкового рівня відповідності $\text{ПчЗВ}(t_0)$.

Приклад 1. Розв'язання задачі

В якості вхідних даних для розрахунків використаємо вміст табл. 4 ($n=8$).

Для обчислення показника планомірності необхідно обчислити дельта-значення відповідності $\Delta\text{ПрЗВ}_{(t_i)}$, $\Delta\text{ПЗВ}_{(t_0,t_i)}$. Розрахунки проводиться за виразом (1). Результати розрахунків наведено в двох нижніх рядках табл. 4.

Використовуючи вирази (5) та (6) з урахуванням значення показника планомірності, розрахуємо:

$$W\left(\Delta\text{ПрЗВ}(t_i),\Delta\text{ПЗВ}(t_0,t_i)\right)=$$

$$=\frac{\sum_{r=1}^{n}\min\left[\Delta\text{прзв}(t_i)_r,\ \Delta\text{пзв}(t_0,t_i)_r\right]}{\sum_{r=1}^{n}\Delta\text{прзв}(t_i)_r}=$$

$$=\frac{5+22+7+1+12+9+5+25}{156}=0{,}55.$$

Розрахований показник планомірності $W\left(\Delta\text{ПрЗВ}(t_i),\Delta\text{ПЗВ}(t_0,t_i)\right)=0{,}55$ вказує на те, що на момент часу t_i планомірність виконання заходів, щодо підвищення ефективності системи управління інформаційною безпекою має оцінку «здійснюється на середньому рівні» зі значенням функції належності, що дорівнює одиниці. Аналогічну оцінку відповідності цільовим значенням в контрольних точках можна отримати шляхом вирішення відповідної задачі.

Приклад вирішення задачі для вирішення відповідності цільового та реального обсягів виконаних заходів з покращення СУІБ представлено нижче.

Приклад 2. Постановка задачі.

Нехай існує організація, в якій здійснюються роботи з впровадження СУІБ згідно з дельта-проміжними цільовими значеннями відповідності $\Delta\text{ПрЗВ}_{(t_i)}$ для n показників безпеки. Необхідно визначити відповідність цільового та реального обсягу виконаних заходів з впровадження СУІБ в момент часу t_i.

Приклад 2. Розв'язання задачі

Для проведення розрахунків як вхідні дані використаємо вміст табл. 5 ($n=8$).

Задача визначення відповідності цільового та реального обсягу виконаних заходів з впровадження СУІБ вирішується за умови відомого значення дельта-поточного значення відповідності вимогам $\Delta\text{ПЗВ}_{(t_0,t_i)}$ у контрольній точці t_i, шляхом обчислення коефіцієнту φ, $0\le\varphi\le N$, де N – розмірність шкали значення відповідності за формулою 3.

$$\varphi=\frac{\#\left(\Delta\text{ПЗВ}_{(t_0,t_i)}\right)}{\#\left(\Delta\text{ПрЗВ}_{(t_i)}\right)}=$$

$$=\frac{62+58+57+38+33+41+71+19}{48+61+59+42+35+50+78+31}=0{,}93.$$

Таблиця 4

Значення областей вимог стандарту ISO/IEC 27001

Області вимог ISO/IEC 27001	$AR-1.1$	$AR-1.2$	$AR-1.3$	$AR-1.4$	$AR-1.5$	$AR-1.6$	$AR-1.7$	$AR-1.8$
$\text{ПЗВ}(t_i)$	56	82	65	91	86	69	70	65
$\text{ПрЗВ}(t_i)$	82	94	81	95	75	69	84	70
$\text{ПчЗВ}(t_0)$	51	60	58	90	63	60	65	40
$\Delta\text{ПЗВ}_{(t_0,t_i)}$	5	22	7	1	12	9	5	25
$\Delta\text{ПрЗВ}_{(t_i)}$	31	34	23	5	5	9	19	30

Таблиця 5

Значення профілів $\Delta\text{ПрЗВ}_{(t_i)}$ та $\Delta\text{ПЗВ}_{(t_0,t_i)}$ організації

ЦЗВ	$AR-1.1$	$AR-1.2$	$AR-1.3$	$AR-1.4$	$AR-1.5$	$AR-1.6$	$AR-1.7$	$AR-1.8$
$\Delta\text{ПрЗВ}_{(t_i)}$	48	61	59	42	35	50	78	31
$\Delta\text{ПЗВ}_{(t_0,t_i)}$	62	58	57	38	33	41	71	19

Розрахований коефіцієнт φ вказує, що реальний обсяг виконаних робіт складає 93% від запланованого на момент часу t_i. Використовуючи обрану шкалу (рисунок 2), можемо стверджувати, що на момент часу t_i програма із впровадження механізмів визначених у ISO/IEC 27001 має оцінку «дуже висока ступінь відповідності» зі значенням функції належності, що дорівнює одиниці.

ВИСНОВКИ

Запропонований підхід дозволяє, використовуючи систему метричних показників, як основу отримання кількісних та якісних значень, що свідчать про стан виконання вимог ISO/IEC 27001, розв'язати такі задачі контролю, як:

– перевірка поточної відповідності вимогам цільовим орієнтирам у контрольних точках;

– перевірка планомірності здійснення заходів з впровадження СУІБ;

– порівняння діяльності з впровадження СУІБ в кількох підрозділах або філіях організації;

– визначення відповідності цільового та реального обсягу виконаних заходів з впровадження СУІБ.

Підхід передбачає виконання робіт, що здійснюються в три етапи:

На першому етапі проводиться вимір відповідності вимогам ISO/IEC 27001 за допомогою розробленої у роботі системи метричних показників.

За результатами отриманих даних вирішуються задачі, що дають змогу отримати результати перевірки обсягів, планомірності та відповідності впровадження заходів підвищення ефективності СУІБ поставленим цілям.

На третьому етапі отримані числові результати інтерпретуються та представляються у вигляді якісної оцінки.

Застосування підходу дозволяє знизити суб'єктивність при проходженні сертифікації за стандартом ISO/IEC 27001, а також спростити роботу внутрішніх аудиторів організації.

Література

[1] ISO/IEC 27001. Information technology – Security techniques – Information security management systems – Requirements. First edition. 2005-10-15.

[2] *Потий А.В.* Классификация показателей безопасности информации [Текст] / А.В. Потий., Д.Ю. Пилипенко. // Системи обробки информации. – Х., 2010. – Вып. 3(84). – С. 53-56.

[3] ISO/IEC 27004. Information technology – Security techniques – Information security management – Measurement. First edition 2009-12-15.

[4] NIST Special Publication 800-55. Information security. Performance Measurement Guide.

[5] *Потій О.В.* Методика оцінки відповідності поточної зрілості цільовим орієнтирам [Текст] /О.В. Потій, А.В. Лєншин //Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – К., 2006. – Вип. (1) 12. – С. 31-43.

Надійшла до редколегії 21.04.2011

Лєншин Анатолій Валерійович, канд. техн. наук, доцент, доцент кафедри БІТ ХНУРЕ. Область наукових інтересів: захист від НСД, захист персональних даних, аналіз ризиків.

Величко Максим Андрійович, магістрант кафедри БІТ ХНУРЕ. Область наукових інтересів: захист інформації в банківських системах.

УДК 681.3.06

Подход к осуществлению контроля внедрения системы управления информационной безопасностью в соответствии ISO/IEC 27001 на основе обработки метрических показателей безопасности методами системного анализа / А.В. Леншин, М.А. Величко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2011. Том 10. № 2. – С. 249–254.

Разработана система показателей безопасности для механизмов защиты из ISO/IEC 27001. Даны постановки задач контроля внедрения СУИБ на основе представления текущих/целевых состояний СУИБ в виде матриц признаков. Предложен метод их решения. Рассмотрены примеры использования разработанного метода.

Ключевые слова: ISO/IEC 27001, показатели безопасности, системный анализ.

Табл. 05. Ил.02. Библиогр.: 05 назв.

UDC 681.3.06

Approach to monitoring implementation of Information Security Management System under ISO/IEC 27001 based on the processing of metric security indicators by system analysis methods / A.V. Lenshyn, M.A. Velychko // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 249–254.

A system of security indicators for ISO/IEC 27001 security mechanisms is developed. The paper provides sets of problems of monitoring implementation of a information security management system (ISMS) on the basis of presenting current/goal ISMS states in the form of feature matrices and a method of their solution. Practical examples of using the method developed are considered.

Keywords: ISO/IEC 27001, security indicators, system analysis.

Tab. 05. Fig. 02. Ref.: 05 items.