

УДК 681.3.06

О.В. Потій<sup>1</sup>, А.В. Леншин<sup>2</sup><sup>1</sup>Харківський університет Повітряних Сил ім. І. Кожедуба, Харків<sup>2</sup>Харківський національний університет радіоелектроніки, Харків

## ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНКИ РИЗИКІВ БЕЗПЕЦІ ІНФОРМАЦІЇ ТА РОЗРОБКА ПРОПОЗИЦІЙ З ЇХ ВДОСКОНАЛЕННЯ НА ОСНОВІ СИСТЕМНОГО ПІДХОДУ

Розглядається сутність методів оцінки ризиків Magerit та MEHARI. Формулюються принципи системного підходу, що мають використовуватися при оцінюванні ризиків безпеці інформації. Описуються методи системного аналізу, що використовуються у методах Magerit та MEHARI. Наводяться результати порівняння досліджуваних методів та формулюються пропозиції щодо синтезу вдосконаленого методу оцінки ризиків безпеці інформації.

**Ключові слова:** безпека інформації, системний підхід, оцінка ризику, синтез.

### Вступ

Однією із найважливіших складових системи управління інформаційною безпекою [1] є оцінювання ризиків (ОР) безпеці інформації (БІ). На відміну від аудиту безпеки, метою якого є визначення ступеня відповідності вимогам певного стандарту в сфері БІ, призначенням процесів ОР є визначення ефективності впроваджених механізмів захисту (МЗ) та формування рекомендацій з поліпшення поточного стану захисту [2]. Оцінювання ризиків БІ не одноразовий захід і має виконуватися на регулярній основі. По суті, оцінювання ризиків БІ є процесом, що дозволяє забезпечити зворотній зв'язок між процесами інвестування в забезпечення БІ та процесами захисту інформації (ПЗІ).

З точки зору процесного підходу (підхід передбачає, що вся діяльність із захисту інформації представляється у вигляді множини взаємопов'язаних ПЗІ) [3] розуміння необхідності оцінювання ризиків БІ приходить до організацій, ПЗІ яких досягли третього рівня зрілості. Крім декларування необхідності захисту інформації у політиці безпеки, наявності множини усталених ПЗІ, та оцінювання того, як ці ПЗІ виконуються, третій рівень зрілості передбачає забезпечення повторюваності та можливості порівняння результатів такого оцінювання [4]. З точки зору авторів статті забезпечення зазначених властивостей можливо на основі використання принципів та методів системного аналізу.

Проведені дослідження публікацій підтверджують цю думку та дозволяють стверджувати, що останнім часом методи та методики оцінки ризиків безпеки інформації набувають все більшу кількість ознак системності як на етапах розробки, так і в ході застосування. Як об'єкт дослідження було обрано процеси оцінювання ризиків БІ згідно двох провідних методів: MEHARI (Франція) [5, 6] та Magerit (Іспанія) [7, 8].

### 1. Сутність методів оцінки ризиків безпеки інформації MAGERIT та MEHARI

Методи оцінки ризиків Magerit та MEHARI є розробками державного органу управління публікаціями Іспанії та французької організації CLUSIF, відповідно. Як впливає з проведеного авторами аналізу, зазначені методи на сьогоднішній день є одними з найбільш деталізованих та методично забезпечених.

#### 1.1. Метод оцінки ризиків Magerit

При проведенні ОР у методі Magerit [7] виконуються такі дії: побудування моделі оцінювання (враховується цінність активів, надається опис залежностей між ними), складання карти ризиків (формалізоване подання загроз, до яких вразливі активи), оцінювання ефективності існуючих МЗ, визначення рейтингу ризиків БІ (класифікація активів за залишковим ризиком БІ), формування звіту з вразливостей, розроблення плану безпеки (визначає процес управління ризиками БІ у відповідних політиках БІ), аналіз вразливостей в інформаційно-телекомунікаційній системі (ІТС) та її окремих складових. Для виконання кожної з дій у Magerit надано відповідний спосіб або метод.

Особливу увагу у Magerit приділяється підбору учасників процесу оцінки ризиків БІ та розподілу функціональних обов'язків між ними. Іншою перевагою методу є можливість використання елементів функціональних профілів захисту, що розробляються згідно рекомендацій ISO/IEC-15408 у якості МЗ [8].

Як головні активи розробники Magerit пропонують розглядати критичну інформацію, як другорядні – сервіси, програмне забезпечення, обладнання, комунікації та персонал. Згідно Magerit оцінки ризиків БІ здійснюється за двофакторною моделлю, що враховує імовірність реалізації загрози та рівень можливих збитків. З урахуванням цього усі МЗ з Magerit поділяються на такі, що зменшують імовірність загрози, та на ті, що зменшують рівень збитків.

Важливою особливістю методу Magerit є розгашене та формалізоване представлення етапів оцінювання ризиків БІ. Це досягається за рахунок чіткого визначення таких елементів процесів оцінювання ризиків БІ як: вхідні дані, вихідні дані, очікувані результати, методи, що використовуються, учасники, що залучаються.

### 1.2. Метод оцінки ризиків МЕНАРИ

Інструментарій МЕНАРИ [5] складається з чотирьох модулів (рис. 1), комплексне використання яких дозволяє адаптувати цей метод до використання у будь-якій організації. Розробники МЕНАРИ пропонують такий порядок проведення ОР: оцінка загрози і її потенціалу, визначення ресурсів, які від неї постраждають, визначення МЗ (п'ять видів), що попередять, захистять або відновлять бізнес процеси організації після реалізації загрози. Для кожного етапу надані прикладні засоби МЕНАРИ [6]: практичні рекомендації, таблиці, розрахункові формули, та шкали оцінок. Супутня документація містить інструкції та поради щодо ефективного використання бази знань (подана у форматі Excel), а також теоретичні відомості щодо управління ризиками БІ. Метод МЕНАРИ використовує трьохфакторну модель ризиків БІ, елементами якої є: імовірність реалізації загрози, рівень вразливості активу до цієї загрози та цінність втраченого активу.

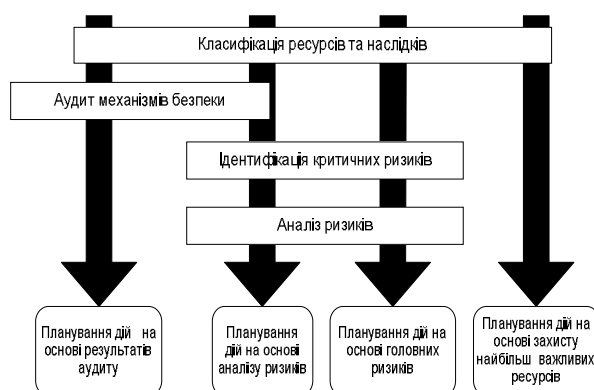


Рис. 1. Модулі МЕНАРИ та чотири підходи до проведення оцінювання ризиків БІ

Для побудови дерева загроз, що є актуальними для ресурсів організації, у методі МЕНАРИ запропоновано використовувати метод сценаріїв. Іншою перевагою МЕНАРИ є наявність шкал оцінювання та способу детермінованого визначення залишкових ризиків БІ. Крім цього, у МЕНАРИ визначено підхід до класифікації активів різних типів та запропоновано таблицю відповідності кращих практик з МЕНАРИ до заходів, що визначені у стандарті ISO/IEC 27002 (наявність такої можливості є безумовно важливою, враховуючи широке застосування ISO/IEC 27002 у сучасній практиці з організації захисту інформації). У МЕНАРИ запропоновані опитувальні листи, що дозволяють оцінити рівень досконалості МЗ, з урахуванням вагових

коефіцієнтів відносної значущості окремих кращих практик, що свідчать про ефективність/досконалість МЗ. Коефіцієнти за замовчуванням можуть бути змінені в ході проведення ОР БІ.

## 2. Застосування системного підходу у ході оцінювання ризиків БІ

### 2.1. Дотримання принципів системного підходу у ході оцінювання ризиків БІ

Забезпечення керованості процесу ОР, а також повторюваності та порівнюваності результатів можливо за рахунок застосування таких принципів системного підходу [9]:

1. Ієрархічність – цілі, що досягаються у результаті виконання процесів ОР мають знаходитись в ієрархічній залежності, тобто кожен рівень цілей має враховувати цілі та чинники, що є актуальними для нього.

2. Декомпозиція – кожен процес ОР має бути представлений у вигляді сукупності підпроцесів. Кожен із підпроцесів повинен мати власні цілі та критерії (метричні показники) своєї ефективності та результативності [10].

3. Достатність та логічна незалежність – логіка організації процесів ОР не повинна залежати від набору кращих практик захисту, МЗ, множини загроз безпеки та множини активів.

4. Модульність та функціональна автономність – має бути виділено окремі модулі (оцінювання активів, оцінювання МЗ тощо), що функціонують незалежно для отримання оцінки ризику БІ.

5. Адаптивність – метод ОР має забезпечувати необхідний рівень ефективності незалежно від умов зовнішнього середовища в якому проводиться оцінювання ризиків БІ.

6. Формалізованість – ОР має забезпечувати отримання зрозумілих (для замовника) кількісних/якісних показників ризику БІ та показників ефективності впровадження МЗ. Опис заходів, що проводяться у ході ОР, повинен виключати неоднозначність тлумачення, тим самим має забезпечуватися повторюваність і порівнюваність результатів оцінки ризиків БІ.

7. Структурованість – дані, що збираються у процесі ОР, мають бути структуровані і подані у вигляді придатному для подальшого використання іншими модулями ОР.

### 2.2. Застосування методів та засобів системного аналізу у ході оцінювання ризиків БІ

Зважаючи на складність проведення ОР та обсяг даних, що мають бути зібрані, актуальною є задача вибору методу опису та представлення як самого процесу ОР, так і компонентів ІТС, що розглядаються як активи організації.

Для розв'язання цієї задачі доцільно використовувати структурні методи – стандартні моделі та методи системного аналізу (СА), що забезпечують

подолання складності великих систем шляхом декомпозиції їх на підсистеми [9].

Традиційно, прикладні методи структурного аналізу поділяють на три групи:

- діаграми, що ілюструють функції, які система повинна виконувати, і зв'язки між цими функціями (DFD, SADT (IDEF0));
- діаграми, що моделюють дані і їх взаємозв'язки (ERD);
- діаграми, що моделюють поведінку системи (STD).

Мабуть найважливіший клас задач, що вирішується у ході ОР є клас задач прийняття рішень. Рішення можуть стосуватися: визначення границь оцінювання, визначення рівня критичності інформаційних ресурсів, вибору пар загроза/інформаційний ресурс, визначення ефективності МЗ тощо. Для підвищення ефективності таких рішень, а також забезпечення порівнюваності та повторюваності результатів оцінки пропонується застосовувати методи підтримки та прийняття рішень. Наприклад, для генерування множини альтернативних рішень, що задовольняють заданим умовам, у СА широко використовуються такі методи як: метод колективної генерації ідей, метод сценаріїв, метод Дельфі, морфологічні методи тощо. Однією з ознак, що можуть використовуватися для класифікації методів оцінювання і вибору альтернатив є кількість критеріїв, що вони дозволяють враховувати. Найкраща альтернатива може обиратися за значенням цільової функції, вид та правила побудови якої визначаються використовуваним математичним апаратом [9].

Для проведення ОР у методах Magerit та МЕНАРИ використовуються такі методи та прийоми СА як: композиція, декомпозиція, прикладні методи функціонального структурного аналізу IDEF-0 та

DFD, експертні методи, метод Дельфі, метод сценаріїв, табличне завдання відповістей, критеріальний метод вибору за результатами бінарного оцінювання.

**IDEF-0** – стандарт, що визначає технологію опису системи у виді множини взаємозалежних дій або функцій. Особливість IDEF-0 - функціональна спрямованість, це дозволяє чітко відокремити аспекти призначення системи від аспектів її фізичної реалізації. Опис системи організований у вигляді ієрархічно впорядкованих та взаємопов'язаних діаграм. Вершину структури займає загальний опис призначення та взаємозв'язок системи з оточуючим середовищем, коріння – найбільш деталізовані описи підлеглих функцій, що виконує система.

Слід відмітити, що ступінь деталізації опису процесів ОР у методі Magerit надає достатні дані для побудовання родини діаграм процесів ОР у нотації IDEF-0. Даними для цього слугують визначені у методі Magerit: структура процесу; продукти кожного етапу; вхідні та вихідні дані; технологія отримання; керівна інформація; функції та обов'язки учасників; перелік виконавців тощо.

У ході дослідження методу Magerit авторами було проведено моделювання процесів ОР. На рис. 2 наведено контекстну діаграму метапроцесу ОР, на рис. 3 – результат моделювання підпроцесу ОР проміжного рівня деталізації.

**DFD** – стандарт для створення моделі потоків інформації, що циркулює в ІТС. Модель системи визначається як ієрархія діаграм потоків даних, що описують асинхронний процес перетворення інформації від введення у систему до отримання користувачем. DFD визначає, яким чином кожний процес перетворює вхідні дані у вихідні та дозволяє виявити співвідношення між процесами.

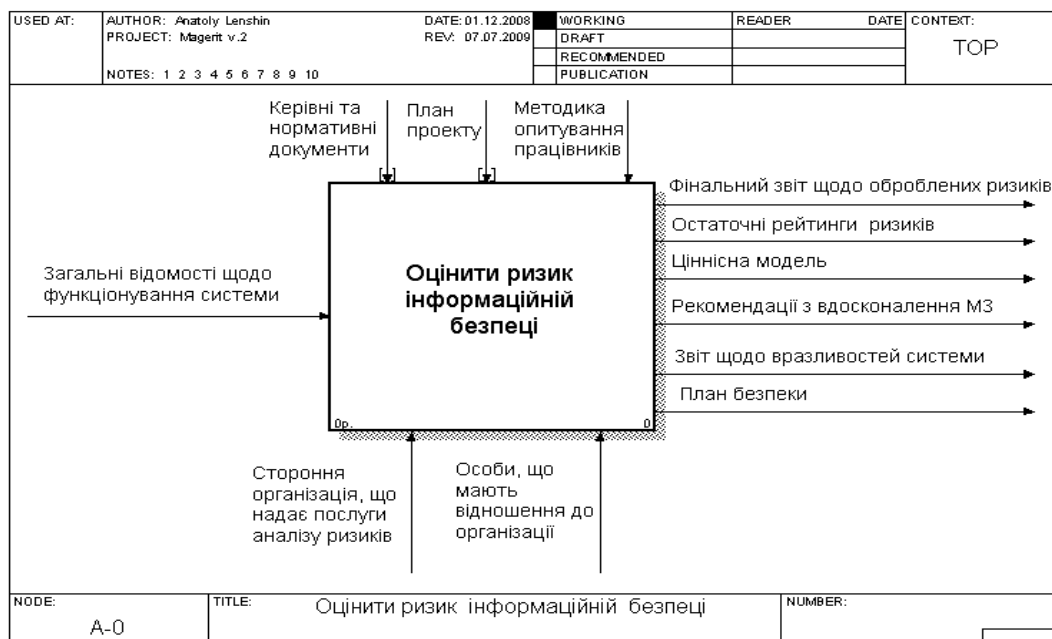


Рис. 2. Контекстна діаграма процесу ОР у нотації IDEF-0

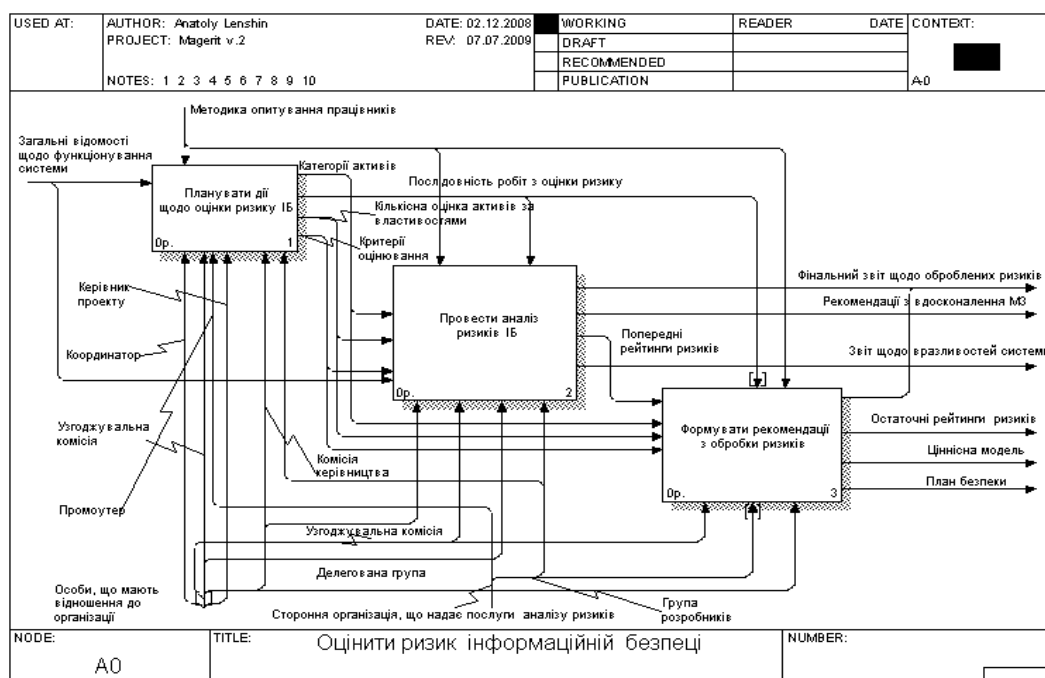


Рис. 3. Декомпозиція метапроцесу ОР у нотації IDEF-0

Розробниками Magerit було запропоновано використовувати DFD на етапі збору інформації, що використовується для визначення цінності активів.

**Метод Дельфі** – складається з кількох етапів, що циклічно повторюються до моменту прийняття компромісного рішення: проведення індивідуальних анкетних опитувань, обробка результатів, ознайомлення експертів із результатами, повторне анкетне опитування.

У Magerit пропонується використовувати метод Дельфі для ідентифікації елементів, що враховуються при оцінці ризиків БІ – активів, загроз, механізмів захисту тощо.

**Метод сценаріїв** передбачає підготовку та узгодження уявлень щодо проблеми або об'єкту, що аналізується, у письмовому вигляді. Зазвичай, текст містить логічну послідовність подій або можливі варіанти вирішення проблеми, впорядковані за хронологією. Сценарій передбачає змістовні міркування, що забезпечують деталізований розгляд проблеми, та результати кількісного техніко-економічного або статистичного аналізу з попередніми висновками, що можна отримати на їх основі. У методі МЕНАРИ запропоновано розвинутий перелік ризик-сценаріїв, що дозволяють провести кількісне оцінювання рівнів ризиків БІ.

**Критеріальний метод** – кожна окрема альтернатива оцінюється одним або кількома показниками. Таким чином, порівняння альтернатив зводиться до обчислення узагальненого показника та порівняння альтернатив за його значенням на основі уведених критеріїв.

**Метод попарного порівняння** – альтернативи (А та В) порівнюються із використанням бінарних оцінок:  $A > B$ , або  $A < B$  або  $A \sim B$ .

### 3. Розробка вдосконаленого методу оцінки ризиків БІ

#### 3.1. Порівняльний аналіз Magerit та МЕНАРИ

За результатами проведених авторами досліджень можна стверджувати, що кожному із методів (Magerit та МЕНАРИ) притаманні певні позитивні риси, які свідчать про системність підходу до проведення ОР. З метою здійснення синтезу вдосконаленого методу на основі Magerit та МЕНАРИ у роботі було проведено порівняння цих методів за такими критеріями: ступінь відповідності стандартам (K1), організація процесів згідно моделі PDCA (K2), модель ризиків, що використовується (K3), вимоги до звітної документації (K4), підтримка методів аналізу вартості проведення ОР (K5), ступінь формалізації алгоритму (K6), суворість вимог до складу аналітичної групи (K7), наявність засобів проведення ОР (K8), види МЗ, що розглядаються (K9), використовувані методи збору даних (K10), наявні критерії оцінки (K11), підхід до обчислення ризику (K12), використовувані методи СА (K13), допоміжне ПЗ (K14). Результати порівняння зведено до табл. 1.

Таблиця 1

Результати порівняння методів ОР Magerit та МЕНАРИ

№	Magerit	МЕНАРИ
K1	Розроблений з урахуванням стандартів BSI. Сумісний з профілями захисту ISO/IEC 15408. Сумісний з ISO/IEC 13335 та ISO/IEC 27001	Повністю відповідає ISO/IEC 27002. Формально відповідає ISO/IEC 13335 та ISO/IEC 27001
K2	Підтримується	Підтримується
K3	Двофакторна: імовірність загрози та рівень наслідків	Трьохфакторна: імовірність загрози, рівень вразливості, рівень наслідків

№	Magerit	МЕНАРИ
K4	По закінченні кожного етапу обов'язково складається документ за визначеною формою	Обов'язковим є розробка політики безпеки. Припускаються записи у довільній формі
K5	Присутні бази для проведення розрахунків	Не підтримуються
K6	Високий, кожний етап має фіксований вхід, вихід та дію	Середній, збираються дані лише для необхідних структур (таблиць)
K7	Чітко визначені	Присутні у загальн. вигляді
K8	Діаграми процесів даних, діаграма цінності активів, типи активів, база МЗ, перелік загроз	Карта природного ризику, карта МЗ, база ризик-сценаріїв, опитувальні листи
K9	2 види: зменшуючи частоту загрози, зменшуючи наслідки	5 видів: попереджуючі, запобіжні, захисні, пом'якшуючі, відновлюючі
K10	Співбесіди з робітниками, опитувальні листи	Опитувальні листи
K11	Критерії для оцінки активів, цінності активів	Критерії для оцінки ризику, статус-ризик
K12	Передбачено розрахунок відхиленого ризику як різниці між базовим та залишковим. Опис алгоритму відсутній	Обчислення з урахуванням множини факторів, передбачає обчислення коефіцієнту вагомості ризику. Наведено опис алгоритму
K13	Експертні методи, метод Дельфі, опис процесів, достатній для побудови IDEF-0 діаграм, DFD	Бальна шкала оцінювання, використання вагових коефіцієнтів, метод сценаріїв
K14	Фрагменти коду для подання даних як XML	База знань МЕНАРИ

### 3.2. Пропозиції щодо організації процесу оцінювання ризиків БІ

Метод Magerit містить формалізовану, ієрархічно структуровану концепцію проведення ОР, визначені обов'язки і ролі учасників ОР. До переваг методу МЕНАРИ слід віднести формалізований модуль оцінки та розгалужену базу ризик-сценаріїв, спосіб класифікації активів, наявність баз даних у вільному доступі. Авторами зроблено спробу висунути вимоги щодо розробки забезпечення для вдосконаленого методу ОР, що матиме переваги Magerit та МЕНАРИ.

1. При формуванні групи учасників ОР слід використовувати рекомендації Magerit. У ході класифікації активів доцільно застосовувати бази знань МЕНАРИ, взявши за основу критерії цінності та оцінки вартості, що запропоновані у методі Magerit.

2. Визначення загроз доцільно проводити за базами Magerit, при цьому обчислювати показники природного ризику слід згідно підходу визначеному у МЕНАРИ.

3. З огляду на детальність опису МЗ у методі МЕНАРИ та наявність таблиць відповідностей з кращими практиками, що визначені у ISO/IEC 27002 (табл. 2), для ідентифікації впроваджених МЗ рекомендується використовувати опитувальні листи МЕНАРИ (табл. 3).

Таблиця 2

Відповідність вимогам стандарту ISO/IEC 27002

Розділ ISO/IEC 27002	Позначення МЗ з МЕНАРИ
5.1 Політика інформаційної безпеки	
5.1.1 Задokumentована політика ІБ	01A02-01
5.1.2 Перегляд політики ІБ	01A02-02
6. Організація інформаційної безпеки	
6.1 Внутрішня організація	
6.1.1 Затвердження концепції ІБ керівництвом	01A02-09
6.1.2 Координація ІБ	01A02-03:05
6.1.3 Розподіл обов'язків з ІБ	01A02-06:07

Таблиця 3

Приклад заповнення елемента опитувального листа з методу МЕНАРИ

01E	Управління безперервністю робочих процесів	Так/ Ні	$w_j^i$	$UL_j^i$	$LL_j^i$
01E01	Питання управління безперервністю бізнесу				
01E01-01	Для визначення засад управління безперервністю бізнесу проведений аналіз критичності застосувань і сервісів. Поглиблений аналіз передбачає існування списку інцидентів і ризик-сценаріїв для визначення наслідків	Ні	4	2	
01E01-02	Аналіз визначає мінімальні системні вимоги для сервісів та застосувань. Системні вимоги узгоджені з власниками/розпорядниками ІР	Так	4	2	3
01E01-03	Для розвитку та оновлення планів безперебійної роботи впроваджені та підтримуються процеси ОР для кожного ІР	Так	2		

4. Оцінювання рівня досконалості МЗ слід виконувати за методом МЕНАРИ згідно з наданими нижче виразами (1) – (4):

$$A_j' = \left( \sum_{i=1}^{k_j} w_j^i y_j^i / \sum_{i=1}^{k_j} w_j^i \right) \times 4, \quad (1)$$

де  $A_j'$  – проміжний рівень досконалості  $j$ -го МЗ,

$w_j^i$  – ненормований ваговий коефіцієнт значущості  $i$ -го твердження для  $j$ -го МЗ,  $y_j^i$  – бінарна оцінка істинності  $i$ -го твердження про досконалість,  $k_j$  – кількість тверджень, що свідчать про досконалість  $j$ -го МЗ.

$$H_j = \min_{i=1,k_j} (UL_j^i), \forall i | y_j^i = 0, \quad (2)$$

де  $UL_j^i$  – максимальний рівень досконалості  $j$ -го МЗ за умови, що  $y_j^i = 0$ .

$$L_j = \max_{i=1,k_j} (LL_j^i), \forall i | y_j^i = 1, \quad (3)$$

де  $LL_j^i$  – мінімальний рівень досконалості  $j$ -го МЗ за умови, що  $y_j^i = 1$ .

$$A_j = \begin{cases} A_j', & L_j \leq A_j' \leq H_j; \\ L_j, & A_j' < L_j; \\ H_j, & A_j' > H_j; \end{cases} \quad (4)$$

де  $A_j$  – рівень досконалості  $j$ -го МЗ.

5. У вдосконаленому методі на етапі оцінювання рівня ризиків рекомендується проводити оцінку залишкового ризику за умови впровадження адекватних МЗ. Це передбачає обчислення статусу потенціалу ризику та статусу наслідків ризику згідно з МЕНАРИ. Розраховане значення позначається як  $S_j(X)$  ( $X = \{DISS, PREV, PROT, PALL, RECUP\}$ ) із попереднім округленням (5):

$$S_j(X) = \begin{cases} 1, & A_j < 1,5; \\ 2, & 1,5 \leq A_j < 2,5; \\ 3, & 2,5 \leq A_j < 3,5; \\ 4, & 3,5 \leq A_j; \end{cases} \quad (5)$$

(DISS – МЗ, що попереджують загрозу, PREV – МЗ, що запобігають, PROT – МЗ, що захищають, PALL – МЗ, що пом'якшують наслідки, RECUP – МЗ, що відновлюють).

Якщо оцінку природної вразливості позначити як STATUS-EXPO, то коефіцієнт зменшення наслідків STATUS-RI розраховується за допомогою матриць оцінювання співвідношення STATUS-PROT, STATUS-RECUP, STATUS-PALL за показниками – конфіденційність, цілісність, доступність. При складанні таблиць враховується можливість розвитку сценарію загроз (таблиця 4). З обчислених показників розраховується коефіцієнт вагомості ризику БІ.

6. Для кожного з проміжних етапів ОР необхідно визначити перелік документації, що є обов'язковою до заповнення (звіти, діаграми, таблиці). Як основу для формування шаблонів (застосування шаблонів значно скорочує часові витрати, та спрощує обробку результатів) доцільно взяти шаблони з Magerit.

Таблиця 4

Робочі таблиці для визначення коефіцієнта STATUS-RI

PROT=1					PROT=2					PROT=3					PROT=4				
R	4	3	3	3	3	R	4	3	3	3	3	R	4	3	3	3	4		
E	3	2	2	3	3	E	3	2	2	3	3	E	3	3	3	3	4		
C	2	1	2	3	3	C	2	1	2	3	3	C	2	2	3	3	4		
U	1	1	2	3	3	U	1	1	2	3	3	U	1	2	3	3	4		
P		1	2	3	4	P		1	2	3	4	P		1	2	3	4		
		P	A	L	L			P	A	L	L			P	A	L	L		

### 3.3. Вимоги до методу оцінки ризиків БІ

Проведені дослідження дозволяють сформулювати такі вимоги до методу оцінки ризиків БІ:

- наявність науково-методичного обґрунтування методів та способів ОР, що використовуються;
- підтримка процесного підходу до організації робіт з ОР;
- підтримка циклу PDCA з ISO/IEC 27001:2005;
- несуперечливість, а краще відповідність вимогам нормативних документів (вітчизняних та міжнародних);
- застосування принципів системності та використання практичних засобів структурного аналізу і методів прийняття рішення;
- можливість адаптації методу ОР до вимог конкретної організації залежно від її типу та розміру;

- можливість отримання результатів у якісному та кількісному виді;
- наявність каталогів: загроз, типів інформації, порушників, механізмів захисту із встановленими на цих множинах відносинах причино-наслідкового зв'язку;
- збір інформації, що буде вихідним матеріалом для формування/редагування концепції захисту та розробки політики безпеки організації;
- простота проведення із можливістю залучення на окремих етапах ОР вузькоспеціалізованих фахівців;
- наочність результатів проведення ОР для замовників;
- наявність модулів, що дозволяють проводити як експрес-оцінювання, так і поглиблене ОР;
- інтегрованість ефективних методів збору даних та роботи з людьми, уникнення громіздкості або надлишковості;

- наявність програмного забезпечення для обробки результатів у повному обсязі із зрозумілим та дружнім інтерфейсом;
- структурованість та модульність складових методу;
- наявність модулю економічного підрахунку вартості проведення ОР та впровадження системи управління інформаційною безпекою;
- наявність модулю економічного обґрунтування доцільності впровадження МЗ;
- придатність до застосування як в існуючих ІТС, так і для ІТС, що розробляються;
- наявність шаблонів для звітних документів.

### Висновки

У організаціях, діяльність із захисту інформації в яких досягла певного рівня зрілості, управління ризиками БІ є невід'ємним елементом СУІБ.

На сьогодні не існує однозначно загально визнаного підходу до проведення ОР. Деякою мірою вирішити це завдання дозволить використання міжнародного стандарту ISO/IEC 27005:2008. Застосуванню цього стандарту на практиці заважає відсутність у ньому конкретних методів, що дозволяють вирішувати задачі притаманні окремим етапам ОР. Аналіз вітчизняної документації свідчить про дуже слабе висвітлення питань керування ризиками і декларування лише загальних принципів.

Іншою нерозв'язаною на сьогодні науково-практичною проблемою є забезпечення повторюваності та порівнюваності результатів ОР. На думку авторів статті, ці властивості можна забезпечити за рахунок застосування системного підходу разом із методами системного аналізу. Це підтверджується тим, що на сьогодні найбільш ефективною формою організації діяльності у сфері захисту інформації є різновид системного підходу – процесний підхід.

Використання у методах Magerit та MEHARI принципу модульності дозволило сформувати про-

позиції щодо організації процесу ОР, який би володів перевагами, що притаманні ОР згідно Magerit та MEHARI.

З метою подальшого розвитку вдосконаленого методу та підвищення адекватності рекомендацій, що формулюються у його результаті, у роботі було висунуто вимоги, яким має задовольняти метод оцінки ризиків БІ.

### Список літератури

1. ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements.
2. ISO/IEC 27005:2008 – Information technology – Security techniques – Information security risk management.
3. Потій О.В. Основні положення системодіальної методології захисту інформації / О.В. Потій, В.Ф. Козак // Прикладна радіоелектроніка – 2007. – Т. 6, № 3, – С. 407-418.
4. Потій О.В. Сутність категорії «зрілість» та змістовна модель зрілості процесів захисту інформації / О.В. Потій // Прикладна радіоелектроніка. Тематичний випуск. – 2006. – Т. 5, № 1. – С. 139-147.
5. MEHARI 2007: Concepts and Mechanisms, Club de la Sécurité de l'Information Français.
6. MEHARI 2007: Knowledge Bases, Club de la Sécurité de l'Information Français.
7. Magerit v2 2006: Book I: The method, Ministerio de Administraciones Publicas, Spain.
8. Magerit v2 2006: Book III: Techniques, Ministerio de Administraciones Publicas, Spain.
9. Спицнадель В.Н. Основы системного анализа: учеб. пос. / В.Н. Спицнадель. – СПб.: «Изд. дом «Бизнес-пресса», 2000. – 326 с.
10. Потій А.В. Показатели оценки безопасности информации / А.В. Потій // 9-я Межд. НТК «Безопасность информации в ИТС»: тез. докл. – К.: ЧП „ЕКМО“, НИЦ „ТЕЗИС“, 2006. – С. 15-16.

Надійшла до редколегії 13.05.2010

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

### ИССЛЕДОВАНИЕ МЕТОДОВ ОЦЕНКИ РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ИХ УСОВЕРШЕНСТВОВАНИЮ НА ОСНОВАНИИ СИСТЕМНОГО ПОХОДА

А.В. Потий, А.В. Леншин

Рассматривается сущность методов оценки рисков Magerit и MEHARI. Формулируются принципы системного подхода, которые должны использоваться при оценке рисков безопасности информации. Описываются методы системного анализа, которые используются в методах Magerit и MEHARI. Приводятся результаты сравнения исследуемых методов и формулируются рекомендации по синтезу усовершенствованного метода оценивания рисков безопасности информации.

**Ключевые слова:** безопасность информации, системный подход, оценка риска, синтез.

### RESEARCH OF INFORMATION SECURITY ASSESSMENT METHODS AND GUIDELINES DESIGN ABOUT ITS IMPROVEMENT ON THE GROUND OF SYSTEM APPROACH

O.V. Potij, A.V. Lenshin

The entity of Magerit and MEHARI methods is considered. Principles of system approach which must use at risks assessment of information security are formulated. System-analysis techniques which used in Magerit and MEHARI methods are described. Comparison results of researching methods are given and recommendations about improvement method synthesis of information security assessment risks are formulated.

**Keywords:** safety of information, approach of the systems, risk estimation, synthesis.