INFORMATION SECURITY RISK MANAGEMENT

DOI: 10.20535/2411-1031.2018.6.2.153494
УДК 004.056.53

ВОЛОДИМИР МОХОР,
ОЛЕКСАНДР БАКАЛИНСЬКИЙ,
ВАСИЛЬ ЦУРКАН

ПРЕДСТАВЛЕННЯ ОЦІНОК РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КАРТОЮ РИЗИКІВ

Розглянуто особливості представлення оцінок ризиків інформаційної безпеки картами ризику. На практиці така карта відображається координатною площино. Її осями позначено параметри ризику інформаційної безпеки. Це ймовірність реалізації загрози та величина втрат. Завдяки цьому визначається прийнятність окремого або групи ризиків інформаційної безпеки. Вона встановлюється шляхом вибору шкали оцінювання (якісної, кількісної або якісно-кількісної); розмірності карти ризику (рівнорозмірна, різнорозмірна). При використанні як рівнорозмірних, так і різнорозмірних карт ризиків інформаційної безпеки здебільшого використовуються лінгвістичні шкали оцінювання (наприклад, “дуже низька”, “низька”, “середня”, “висока”, “дуже висока”). Такий підхід обмежується складністю зіставлення вірогідних оцінок параметрів ймовірності реалізації загрози та величини втрат. Це призводить до проблематичності визначення прийнятності оцінок ризиків інформаційної безпеки і, як наслідок, прийняття рішення про необхідність їх оброблення. Дане обмеження долається шляхом поєднання лінгвістичних і порядкових шкал. Поєднання шкал дозволяє подолати обмеженість зіставлення оцінок ризиків інформаційної безпеки та встановити чіткі межі на карті. Використання дискретних карт з чіткими (дискретними) межами доповнюється кольоровими позначеннями. Зеленим кольором виокремлюються прийнятні оцінки, червоним – неприйнятні. Рівень прийнятності задається експертом і залежить від його знань, навичок, підготовленості та досвіду. Адекватність використання дискретних карт ризиків інформаційної безпеки визначається її розмірністю. Тому за потреби можливе її підвищення. З одного боку можливе врахування проміжних значень величини ризику інформаційної безпеки. Тоді як, з іншого, призведе до перебору великої кількості пар (ймовірність реалізації загрози, величина втрат), складнощів їх сприйняття і зростання часу для прийняття рішення про доцільність/недоцільність оброблення неприйнятних ризиків інформаційної безпеки. Таким чином, використання дискретних карт обмежене складнощами, по-перше, оцінювання, зіставлення і врахування пар (ймовірність реалізації загрози, величина втрат). Врахування цих складнощів можливе завдяки представленню оцінок ризиків інформаційної безпеки неперервними картами.

Ключові слова: ризик інформаційної безпеки, оцінка ризику інформаційної безпеки, шкала оцінювання, карта ризиків, дискретна карта ризиків, неперервна карта ризиків.

Постановка проблеми. Системне, наочне представлення оцінок ризиків інформаційної безпеки здійснюється шляхом використання карти. Традиційно вона відображається як координатна площина, осями якої є параметри ризику. В більшості випадків – це ймовірність реалізації загрози і величина ймовірних втрат [1], [2]. Осями координат в картах ризиків є шкали, що розробляються і використовуються ризик-менеджерами для оцінювання ризиків. Карти ризиків зручно використовувати для їх моніторингу, коли за результатами його проведення ризики “наносяться” на координатну площину, і перегляд карт в динаміці дозволяє візуально системно уявити тенденції їх зміни. Вони можуть складатися для всієї організації, для окремих процесів, напрямків, структурних підрозділів організації, для окремих груп ризиків.

Застосування універсальної (однотипної) форми карти для груп ризиків, підрозділів і всієї організації дозволяє об'єднувати, порівнювати, накладати, інтегрувати карти ризиків. Це забезпечує отримання нової інформації про ризики інформаційної безпеки організації, необхідної для проведення аналізу і прийняття рішень про керування ними [1], [3].

Аналіз останніх досліджень і публікацій. Способам представлення оцінок ризиків інформаційної безпеки приділено уваги в [3] - [10]. Зокрема, розглянуто окремі аспекти їх представлення. Наприклад [6] - [10], деревом ризиків; використання кругових діаграм; карт ризиків з дискретними шкалами оцінок параметрів ризику. Однак [7], [10], Серед них найбіль розповсюдженим способом є представлення оцінок ризиків інформаційної безпеки картою. Карти умовно поділяються на карти ризиків загального виду та прикладні карти ризиків. Карти загального виду можуть використовуватися без шкал оцінювання. Це дозволяє використовувати даний різновид для будь-яких ризиків. При цьому, відсутність шкал компенсується зазначенням областей оцінок ризику. Наприклад [8], області низького, нижче середнього, середнього, вище середнього і високого ризику, близького до критичного. Для кожної із зазначених областей встановлено інтервальні значення обраних параметрів ризику (ймовірності реалізації загрози та величини втрат) [10]. Тоді як особливістю прикладних карт ризиків є нанесення параметрів ризику інформаційної безпеки організації за їх кількісною оцінкою [7].

Метою статті є аналізування способу представлення оцінок ризику інформаційної безпеки картою.

Виклад основного матеріалу досліджень. Оцінка ризиків інформаційної безпеки відображається на карті як результат множення ймовірності реалізації загрози та величини втрат. При цьому власник організації за власний розсуд повинен визначити критерії прийнятності. Здебільшого, не до кінця розуміючи, що саме цей критерій визначає, які саме втрати і в яких одиницях є прийнятними для діяльності його організації, а які стають вже критичними. Таким чином, подібний спосіб задання вимог для системи управління інформаційною безпекою, яку проектують, має ряд недоліків. В першу чергу це дискретність кроку зміни значень величини ризику. Зокрема, викликають складнощі тлумачення діапазононів таких змін, наприклад, від 12 до 20. Наслідоком цього є залежність вибору заходів обробляння ризиків та складових системи управління інформаційною безпекою від суб'єктивної точки зору фахівця, залежність від суджень експертів, відсутність інших формальних вимог до проектування означеної системи [7], [8], [10].

Тому для використання карт ризиків необхідно визначити їх розмірність. Карта ризику може вибиратись рівнорозмірною (типу *nxn*), так і різнорозмірною (типу *nxm*). Як правило, при побудові такої карти, у лівому стовпчику відображаються значення ймовірності реалізації загрози виражені у лінгвістичних і порядкових. За аналогією, у верхньому рядку записуються значення вартості можливих втрат у випадку, якщо ризик реалізовується та такі наслідки настають. На перетині стовпчиків та рядків отримується добуток значень стовпчиків та рядків і, як наслідок, оцінка ризику інформаційної безпеки [7], [10].

Рівнорозмірні карти ризиків типу nxn. Приклад застосування лінгвістичних значень ризиків. Розглянемо приклад тільки якісного завдання імовірності реалізації загрози та вартості втрат. Надаємо їм наступні лінгвістичні значення за зростанням величини: "Дуже низька", "Низька", "Середня", "Висока", "Дуже висока" (див. рис. 1). На перетині рядків та стовпчиків є комбінації лінгвістичних значень типу, наприклад: "Дуже низька·/ Дуже висока", "Дуже висока·/ Дуже висока". Такі комбінації оцінити досить складно, а ще складніше зіставити такі результати з конкретним станом справ та розкриттям семантичного змісту. Отримання добутку лінгвістичних змінних ризику потребує застосування теорії нечітких множин що, за відсутності відповідної статистики ускладнен. Перехід до чітких визначень оцок імовірності, або ступеню впливу здійснюється якщо при застосуванню лінгвістичної шкали оцінок до кожного логічного терму відповідає класична чітка оцінка (1, 2, 3, ...), яка і буде визначати одну з меж (ліву або праву) інтервалу оцінювання у випадку нечітких знань експертів. При цьому, якщо знання (оцінки) є чіткими, то права границя буде співпадати з лівою [7] - [10].

Ймовірність інцидентного сценарію / Ступень впливу	Дуже низька	Низька	Середня	Висока	Дуже висока
Дуже висока	ДНхДВ	НхДВ	Сх	Вх	ДВх
Висока	ДНхВ	НхВ	СхВ	ВхВ	ДВхВ
Середня	ДНхС	НхС	СхС	ВхС	ДВхС
Низька	ДНхН	НхН	СхН	ВхН	ДВхН
Дуже низька	ДНхДН	НхДН	СхДН	ВхДН	ДВхДН

Рисунок 1 – Вигляд “Карти ризиків” при задаванні лінгвістичних критеріїв

В такому випадку на перетині кожного стовпчика та кожного рядку записується добуток значень, які надані відповідному стовпчику, і відповідному рядку виходячи з визначення ризику. Для візуального поділу множини ризиків на підмножини прийнятних та неприйнятних ризиків, використовуються такі кольорові позначення: зеленим визначаються прийнятні ризики, червоним – неприйнятні. Таким чином, цей спосіб залежним від знань, навичок, рівня підготовки та досвіду експертів.

Приклад застосування карти ризиків розміром 5х5. Розглянемо порядок виконання вимоги щодо визначення ризиків, які необхідно взяти до уваги при проектуванні системи управління інформаційною безпекою на прикладі карти розміром 5х5 із застосуванням лінгвістичних (якісних) значень, та їх чіткої кількісної оцінки [7], [8]. На рис. 2 як критерій прийнятності визначено показник рівня ризику, який відповідає вимозі: більше рівня “Дуже низький”. Для того, щоб знайти множину ризиків, які відповідають такій вимозі, необхідно на перетині стовпчика та рядка, які відповідають значенню “Дуже низька” знайти значення величини ризку, яке у цьому випадку дорівнює “1”. Далі необхідно порівняти його зі значеннями ризиків, які знаходяться у інших клітинах. Після порівняння, можна впевнились, що в таблиці інших значень, які б задовольняли немає. Тобто робимо висновок, що при заданому критерії “Більше рівня “Дуже низький” для проектування системи управління інформаційною безпекою необхідно враховувати 24 оцінки ризику.

На наступному етапі розглянемо послідовність дій при заданні критерію: врахувати ризики, значення яких більше рівня “Низький”, рис. 2. Визначимо, що на перетині стовпчика та рядка зі значенням “Низька” отримуємо значення “4”. Це значення визначає максимальну оцінку ризику, що не враховується при проектуванні системи управління інформаційною безпекою, при заданні критерію “Врахувати ризики, значення яких більше рівня “Низький”. Порівнюючи значення ризиків у кожній клітинці на карті ризиків, знаходимо всі значення ризиків, величина яких дорівнює, або менша “4”. Таких у таблиці 8. Тобто при проектуванні системи управління інформаційною безпекою враховуються тільки 17 оцінок.

Ймовірність інцидентного сценарію / Ступень впливу	Дуже низька 1	Низька 2	Середня 3	Висока 4	Дуже висока 5
Дуже висока 5	5	10	15	20	25
Висока 4	4	8	12	16	20
Середня 3	3	6	9	12	15
Низька 2	2	4	6	8	10
Дуже низька 1	1	2	3	4	5

Рисунок 2 – Вигляд “Карти ризиків” при визначенні критерію: врахувати ризики, які більше рівня “Дуже низький”

Ймовірність інцидентного сценарію / Ступень впливу	Дуже низька 1	Низька 2	Середня 3	Висока 4	Дуже висока 5
Дуже висока 5	5	10	15	20	25
Висока 4	4	8	12	16	20
Середня 3	3	6	9	12	15
Низька 2	2	4	6	8	10
Дуже низька 1	1	2	3	4	5

Рисунок 3 – Вигляд “Карти ризиків” при визначенні критерію: врахувати ризики, значення яких більше рівня “Низька”

На рис. 4 і 5 розглядаємо випадки задання критеріїв: більше рівня “Середня” та більше рівня “Висока”. У випадку “більше рівня “Середня”” необхідно враховувати 10 оцінок ризиків, а при критерії “більше рівня “Висока” – 3. Прослідковується закономірність, що кожний наступний крок здійснюється по лінії, яка визначає значення квадратів оцінок ризику.

Ймовірність інцидентного сценарію		Дуже низька	Низька	Середня	Висока	Дуже висока
Ступень впливу		1	2	3	4	5
Дуже висока	5	5	10	15	20	25
Висока	4	4	8	12	16	20
Середня	3	3	6	9	12	15
Низька	2	2	4	6	8	10
Дуже низька	1	1	2	3	4	5

Рисунок 4 – Вигляд “Карти ризиків” при визначенні критерію: врахувати ризики, значення яких більше рівня “Середня”

Ймовірність інцидентного сценарію		Дуже низька	Низька	Середня	Висока	Дуже висока
Ступень впливу		1	2	3	4	5
Дуже висока	5	5	10	15	20	25
Висока	4	4	8	12	16	20
Середня	3	3	6	9	12	15
Низька	2	2	4	6	8	10
Дуже низька	1	1	2	3	4	5

Рисунок 5 – Вигляд “Карти ризиків” при визначенні критерію: врахувати ризики, значення яких більше рівня “Висока”

З огляду на це, можна зробити висновок, що в залежності від зростання оцінок імовірності та величини втрат зростає крок (відстань). Ця відстань визначається шляхом віднімання від значень більшого ризику значення меншого (попереднього). Кожна наступна оцінка ризику все більше. Така дискретність не дає можливості враховувати ризики, значення яких можуть знаходитись між попереднім та наступним за ним критерієм, наприклад між 9 та 12 міститься 10 та 11, а між 20 та 25 - 21, 22, 23, 24. Для врахування таких значень можна підвищити розмірність карти ризиків зі сподіванням отримати більш адекватну карту ризиків, яка врахує проблеми, які пов’язані з дискретністю [7], [10].

Однак, при підвищенні розмірності карти ризиків необхідно здійснювати повний перебір всіх значень з метою впевнитись чи всі ризики, які необхідно враховувати, дійсно менші, ніж заданий критерій (наприклад, для карти 10x10, необхідно врахувати 100 значень). Такий перебір обумовлений втратами часу, а при підвищенні кратності карти ризиків – часу, який необхідний для здійснення такого перебору (див. рис. 6). Тобто, за допомогою збільшення кратності карти ризиків, більш адекватно враховувати всі значення ризиків, які існують, невиправдано зростає час для проведення таких порівнянь, що після перевищення певного значення кратності починає негативно впливати на розроблення системи управління інформаційною безпекою [8], [10].

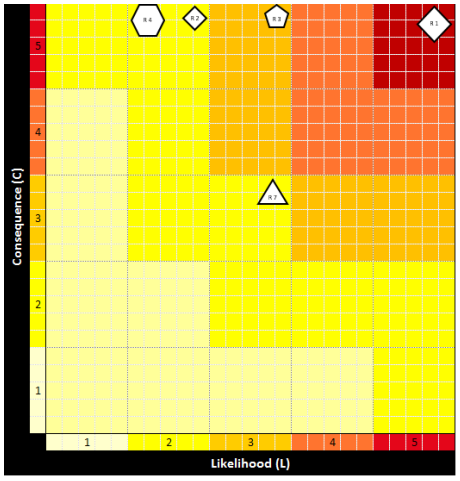

Рисунок 6 – Вигляд “Карти ризиків” при підвищенні її кратності

Підвищення кратності карт ризиків може спонукати до використання неперервних карт, які застосовуються, наприклад у медицині (див. рис. 7).

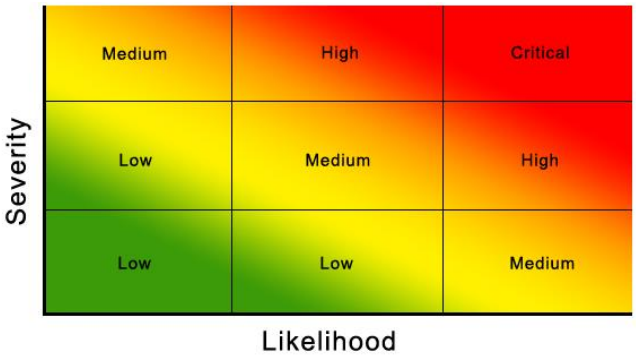

Рисунок 7 – Вигляд неперервних карт ризиків

Розглянемо наступний приклад (див. рис. 8) виконання вимоги “Врахувати всі ризики, значення яких знаходяться між 28 та 32”. Для зручності значення ризиків, які менше та дорівнюють 28 позначимо зеленим кольором, значення, які дорівнюють 32 та вище - жовтим.

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	28	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

Рисунок 8 – Врахувати ризики, значення яких знаходиться між “28” та “32”

З огляду на рис. 8, доцільно звернути на чотири випадки, які відповідають рівню “30”. Але взагалі не зрозуміло, що робити у випадку, коли ризик повинен дорівнювати 31? А в заданому діапазоні з 28 до 32 міститься три цілих числа (29, 30, 31), як враховувати їх? Ця проблема теж не має рішення, тому що, як було сказано раніше, спроба підвищити розмірність таблиці призведе до невиправданих витрат часу або до похибок оцінювання ризиків. Нагадаємо [1], [3], [4] що за розробку та подальше використання методики оцінювання ризиків відповідальність несе перша особа організації, яка повинна обрати та затвердити методику їх оцінювання та визначити рівень прийнятності ризиків інформаційної безпеки. До того ж, виникає питання, в якій мірі неспівмірність діапазонів шкал може вплинути на спосіб задання прийнятності ризику та якість отриманих результатів. Для вирішення цього питання розглянемо випадок використання різнорозмірних карт ризиків, наприклад, 3x5.

Різнорозмірні карти ризиків типу *nxm*. Приклад застосування різнорозмірних “карт ризиків”. У цьому випадку будемо у кожному наступному варіанті підвищувати рівень максимально прийнятного ризику. Для цього скористаємось аналогією з попереднім прикладом та отримаємо такі значення: 1, 3, 9. На рис. 9 наведемо приклад визначення ризиків, значення яких більше “9” [7], [8], [10].

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21

Рисунок 9 – Вимога: врахувати ризики, рівень яких вище ніж “9”

Однак, для завдавання рівнів прийнятних ризиків, принцип задання треба змінювати. Наприклад, на рис. рис. 10-12 найбільш прийнятним ризиком є кожне наступне число, за зростанням, яке слідує за попереднім у таблиці – 10, 12, 14.

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21

Рисунок 10 – Вимога: врахувати ризики, які більше ніж “10”

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21

Рисунок 11 – Вимога: врахувати ризики, які більше ніж “12”

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21

Рисунок 12 – Вимога: врахувати ризики, які більше ніж “14”

Отже, при застосуванні такого підходу необхідно перебирати всі можливі варіанти величини ризиків. Спочатку здійснюється пошук найбільшого для конкретної ітерації значення прийнятного ризику, а потім воно порівнюється з іншими значеннями. Завдяки цьому виокремлюється множина неприйнятних ризиків, що враховуються при розробленні системи управління інформаційною безпекою.

Ще одним варіантом задавання рівня прийнятного ризику є побудова діагоналі, за аналогією діагоналі, на якій розміщуються значення n^2 (див. рис. 13). На карті з нерівномірним розподілом значень величини ризиків, її побудова здійснюється на власний розсуд без математичного обґрунтування [7]. Це вказує на залежніть такого відображення від суб’єктивних поглядів експертів.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	8	10	12
3	3	6	9	12	15	18
4	4	8	12	16	20	24

а)

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	8	10	12
3	3	6	9	12	15	18
4	4	8	12	16	20	24

б)

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	8	10	12
3	3	6	9	12	15	18
4	4	8	12	16	20	24

в)

Рисунок 13 – Нерівномірна карта ризику з нечіткою діагоналлю

Таким чином, при використанні карт ризику виду *nxm* виникає ще більше складнощів, ніж для рівно розмірних карт. Наприклад, звернемо увагу на рис. 14. На осі абсцис відкладено значення ймовірності у відсотках, а на осі ординат – вірогідні втрати, виражені у мільйонах гривень. Криві на картах розмежовують різні категорії ризиків, але, як співвідносяться величини 100% та 16000 не зрозуміло. Водночас виникає питання стосовно можвлиовсті їх зіставлення і типу кривих.

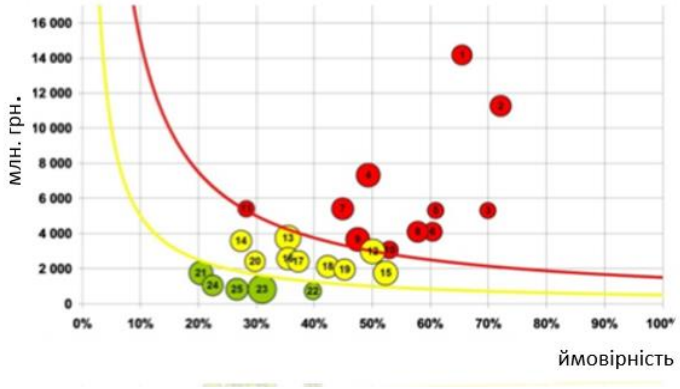

Рисунок 14 – Прикла різнорозмірної карти ризиків

Для уникнення означених складнощів, зазвичай проводиться нормування значень параметрів ризику. Для цього необхідно представити ймовірність та збитки в однакових одиницях. Наприклад, якщо ймовірність реалізації загрози може знаходитись в межах від 1% до 100%, то збитки теж доцільно оцінювати в таких же одиницях. Тоді для прикладу рис. 14, значення 100 умовних одиниць дорівнює 16 000 млн.грн.. Таким чином, одна умовна одиниця дорівнює 160 млн. грн. Очевидним є факт, що максимальне значення ризику дорівнюватиме 100. Такий підхід дає можливість привести карту розмірності *nxm* до карти розмірності *nxn*. Зрозумілим є і той факт, що після отримання результатів оцінювання ризиків, здійснених у нормованих величинах, необхідно здійснювати обернене перетворення.

Висновки. Розглянувши існуючі способи представлення ризиків при розробленні системи управління інформаційною безпекою за допомогою карти встановлено:

1. При використнні “Карти ризиків” зі заданими лінгвістичними критеріями, отримані комбінації лінгвістичних значень оцінити дуже складно.
2. Зіставлення значень лінгвістичних величини з конкретним станом інформаційної безпеки або рівнем ризику практично неможливий.
3. При застосуванні карт ризиків із кількісними оцінками ймовірності та величини втрат існує дискретність та нерівномірність кроку значень ризиків. Це призводить до складнощів виконання вимоги щодо врахування всіх ризиків.
4. Для запобігання зростанню кількості неврахованих ризиків, застосовується збільшення розмірності таблиці. Проте, такий підхід тягне за собою зростання загальної кількості значень ризиків у таблиці. Це призводить до зростання кількості ітерацій порівняння рівня заданого максимально прийнятного ризику з усіма значеннями ризиків карти. Тому зростає час, який необхідно витратити на розділення множини ризиків на підмножини прийнятних і неприйнятних ризиків.
5. При застосуванні карт ризику виникає необхідність нормувати не зіставні оцінки ймовірності та величини втрат, які задаються у різних одиницях (наприклад: відсотках і гривнях, частках або долях і тисячах) та здійснювати обернене перетворення.
6. Карти ризиків використовуються для визначення, класифікації та ранжування вірогідних ризиків з метою мінімізації витрат на їх оброблення. Тому на картах ризиків доцільно правильно розподіляти можливі ризики за категоріями. Наприклад, прийнятні ризики – в зеленій зоні, в жовтій – ризики, які необхідно постійно контролювати, а в червоній – неприйнятні ризики.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements.* [Online]. Available: https://www.iso.org/standard/54534.html.

[2] International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27002. Information technology. Security techniques. Code of practice for information security controls*. [Online]. Available: https://www.iso.org/standard/54533.html.

[3] International Organization for Standardization. (2011, June 10). *ISO/IEC 27005. Information technology. Security techniques. Information security risk management.* [Online]. Available: https://www.iso.org/standard/56742.html.

[4] International Organization for Standardization. (2018, Febr. 15). *ISO 31000. Risk management. Guidelines.* [Online]. Available: https://www.iso.org/standard/65694.html.

[5] International Organization for Standardization. (2009, Nov. 27). *IEC 31010. Risk management. Risk assessment techniques.* [Online]. Available: https://www.iso.org/standard/51073.html.

[6] А. Г. Бадалова, и А. В. Пантелеев, Управление рисками деятельности предприятия. Москва, Российская Федерация: Вузовская кника, 2016.

[7] В. Мохор, О. Бакалинський, та В. Цуркан, "Аналіз способів представлення оцінок ризиків інформаційної безпеки", Information Technology and Technology, vol. 6, iss. 1, 2018.
doi: 10.20535/2411-1031.2018.6.1.153189.

[8] С. А. Петренко, и С. В. Симонов, Управление информационными рисками. Экономически оправданная безопасность. Москва, Российская Федерация: Компания АйТи; ДМК Пресс, 2004.

[9] Я. Д. Вишняков, и Н. Н. Радаев, Общая теория рисков. Москва, Российская Федерация: Издательский центр "Академия", 2007.

[10] А. М. Астахов, Исскуство управления информационными рисками. Москва, Российская Федерация: ДМК Пресс, 2010.

Стаття надійшла до редакції 5 вересня 2018 року.

REFERENCE

[1] International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements.* [Online]. Available: https://www.iso.org/standard/54534.html.

[2] International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27002. Information technology. Security techniques. Code of practice for information security controls*. [Online]. Available: https://www.iso.org/standard/54533.html.

[3] International Organization for Standardization. (2011, June 10). *ISO/IEC 27005. Information technology. Security techniques. Information security risk management.* [Online]. Available: https://www.iso.org/standard/56742.html.

[4] International Organization for Standardization. (2018, Febr. 15). *ISO 31000. Risk management. Guidelines.* [Online]. Available: https://www.iso.org/standard/65694.html.

[5] International Organization for Standardization. (2009, Nov. 27). *IEC 31010. Risk management. Risk assessment techniques.* [Online]. Available: https://www.iso.org/standard/51073.html.

[6] A. G. Badalova, and A. V. Panteleev, *Risk management of the enterprise*. Moskow, Russia: Vuzovskaia knika, 2016.

[7] V. Mokhor, O. Bakalynskyi, and V. Tsurkan, "Analysis of information security risk assessment representation methods", Information Technology and Technology, vol. 6, iss. 1, 2018.
doi: 10.20535/2411-1031.2018.6.1.153189.

[8] S. A. Petrenko, and S. V. Simonov, Information risk management. Cost-effective security. Moskow, Russia: DMK Press, 2004.

[9] I. D. Vishniakov, and N. N. Radaev, General risk theory. Moskow, Russia: Publ. “Akademiia”, 2007.
[10] A. M. Astakhov, The art of information risk management. Moskow, Russia: DMK Press, 2010.

ВЛАДИМИР МОХОР,
АЛЕКСАНДР БАКАЛИНСКИЙ,
ВАСИЛИЙ ЦУРКАН

ПРЕДСТАВЛЕНИЕ ОЦЕНОК РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАРТОЮ РИСКОВ

Рассмотрены особенности представления оценок рисков информационной безопасности картами риска. На практике такая карта отображается координатной плоскостью. Ее осями обозначаются параметры риска информационной безопасности. Это вероятность реализации угрозы и величина потерь. Благодаря этому определяется приемлемость отдельного или группы рисков информационной безопасности. Она устанавливается путем выбора шкалы оценивания (качественной, количественной, качественно-количественной), размерности карты риска (равноразмерная, разноразмерная). При использовании как равноразмерных, так и разноразмерных карт рисков информационной безопасности в большинстве случаев используются лингвистические шкалы оценивания (например «очень низкая», «низкая», «средняя», «высокая», «очень высокая»). Такой подход ограничивается сложностью сопоставления возможных оценок параметров вероятности реализации угрозы и величины потерь. Это приводит к проблематичности определения приемлемости оценок рисков информационной безопасности и, как следствие, принятия решений о необходимости их обработки. Данное ограничение преодолевается путем сочетания лингвистических и порядковых шкал. Сочетание шкал позволяет преодолеть ограниченность сопоставления оценок рисков информационной безопасности и установить четкие границы на карте. Использование дискретных карт с четкими (дискретными) границами дополняется цветными обозначениями. Зеленым цветом выделяются приемлемые оценки, красным – неприемлемые. Уровень приемлемости задается экспертом и зависит от его знаний, навыков, подготовленности и опыта. Адекватность использования дискретных карт рисков информационной безопасности определяется ее размерностью. Поэтому в случае необходимости возможное ее повышение. С одной стороны возможен учет промежуточных значений величины риска информационной безопасности. Тогда как, с другой, приведет к перебору большого количества пар (вероятность реализации угрозы, величина потерь). Учет этих трудностей возможен благодаря представлению оценок рисков информационной безопасности непрерывными картами.

Ключевые слова: риск информационной безопасности, оценка риска информационной безопасности, шкала оценивания, карта рисков, дискретная карта рисков, непрерывная карта рисков.

VOLODYMYR MOKHOR,
OLEKSANDR BAKALYNSKYI,
VASYL TSURKAN

RISK ASSESSMENT PRESENTATION OF INFORMATION SECURITY BY THE RISKS MAP

The risk assessment presentation features of information security by the risk maps are considered. In practice, such map is displayed on the coordinate plane. Its axes denote information security risk parameters. This is the risks and the losses magnitude. This determines the acceptability of separate or group information security risks. It is established by choosing the scale

of assessment (qualitative, quantitative, or qualitative-quantitative); risk map dimensionality (equal in size, different in size). When used risks maps of information security equally in size and different in size, linguistic rating scales mainly apply (for example, “very low”, “low”, “medium”, “high”, “very high”). This approach is limited by the complexity of comparing possible parameters estimates of risk possibility and the losses magnitude. This leads to the difficulty of determining the information security risk assessments acceptability and, as a result, the decision to process them. This limitation is overcome by a combination of linguistic and ordinal scales. The combination of scales allows overcoming the comparing information security risk assessments limitations and establishing clear boundaries on the map. The use of discrete maps with clear (discrete) limits is complemented by color symbols. Acceptable assessments highlight in green, unacceptable in red. The level of acceptability is established by the expert and depends on his knowledge, skills, preparedness, and experience. The adequacy of using discrete information security risk maps is determined by its dimensionality. Therefore, if necessary, it can be increased. On the one hand, it is possible to take into account the intermediate values of the information security risk. On the other hand, it will lead to the enumeration of a large number of pairs (risks, the losses magnitude), difficulties of their perception and the increase in time for deciding whether or not to handle unacceptable information security risks. Thus, the use of discrete maps is limited by the difficulties, firstly, the assessment, comparison and accounting of pairs (the probability of the risks, the losses magnitude). Accounting for these difficulties is possible through the presentation risk assessment of information security by the continuous map.

Keywords: information security risk, information security risk assessment, rating scale, risk map, discrete risk map, continuous risk map.

Володимир Володимирович Мохор, член-кореспондент Національної академії наук України, доктор технічних наук, професор, директор, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

ORCID: 0000-0001-5419-9332.

E-mail: v.mokhor@gmail.com.

Олександр Олегович Бакалинський, начальник відділу, Департамент формування та реалізації державної політики у сфері кіберзахисту Державної служби спеціального зв’язку та захисту інформації, Київ, Україна.

ORCID: 0000-0001-9712-2036.

E-mail: baov@meta.ua.

Василь Васильович Цуркан, кандидат технічних наук, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України ”Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.

ORCID: 0000-0003-1352-042X.

E-mail: v.v.tsurkan@gmail.com.

Владимир Владимирович Мохор, член-корреспондент Национальной академии наук Украины, доктор технических наук, профессор, директор, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Александр Олегович Бакалинський, начальник отдела, Департамент формирования и реализации государственной политики в сфере киберзащиты Государственной службы специальной связи и защиты информации, Киев, Киев, Украина.

Василий Васильевич Цуркан, кандидат технических наук, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины “Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.

Volodymyr Mokhor, corresponding member of the National Academy of Sciences of Ukraine, doctor of technical sciences, professor, director, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.

Oleksandr Bakalynskyi, head of department, Department of formation and implementation of state policy on cyber protection of Administration of state serves of special communication and information protection of Ukraine, Kyiv, Ukraine.

Vasyl Tsurkan, candidate of technical sciences, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.