УДК 004.056

А. В. Скиба,
аспірант, НТУУ "КПІ"
О. Є. Архипов,
д. т. н., професор кафедри інформаційної безпеки НТУУ "КПІ"

МЕТОД УПРАЛІННЯ ЗАГАЛЬНИМ СТАНОМ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ ЗА ДОПОМОГОЮ АНАЛІЗУ ПРИЧИННО-НАСЛІДКОВИХ ВЗАЄМОЗВ'ЯЗКІВ ЗА МЕТОДОМ ІСІКАВИ

A. Skyba,
PhD student NTUU "KPI"
O. Arkhypov,
Dr. Sci. Tech., NTUU "KPI"

THE METHOD OF INFORMATION SECURITY MANAGEMENT BY ANALYZING THE CAUSAL RELATIONSHIPS BY ISHIKAWA METHOD

Розглядається метод управління загальним станом захищеності інформаційної безпеки компанії за допомогою аналізу причинно-наслідкових взаємозв'язків за методом Ісікави задля підвищення якості управління інформаційною безпекою підприємства. Для проведення адекватного оцінювання інформаційних ризиків та оптимізації обсягів інвестицій в інформаційну безпеку застосовуються підходи та процедури, що спираються на існуючі міжнародні стандарти з менеджменту ризиків інформаційної безпеки. На жаль, ці стандарти мають переважно концептуально-рекомендаційний характер і не враховують багатьох факторів, котрі суттєво впливають на точність та об'єктивність оцінювання ризиків. Метод визначення загального стану захищеності за допомогою аналізу причинно-наслідкових взаємозв'язків за методом Ісікави дає можливість врахувати як фактори небезпеки зловмисника, так і фактори захисту самої компанії, а також за допомогою економіко-вартісного підходу до аналізу ризиків, надати інформацію щодо втрат та інвестицій в інформаційну безпеку. Запропонований метод використовує соціально-психологічні та мотиваційні показники особистостей зловмисника, технічні параметри об'єктів, інформацію про компанію та фінансові можливості, що дозволяє проводити комплексну оцінку. Даний метод дозволяє об'єднати як мінімальну, так і необхідну кількість показників для оптимізації дослідження інформаційних та фінансових ризиків. Запропонований метод завдяки простій масштабованості забезпечує покриття всіх необхідних показників для комплексної оцінки стану захищеності інформаційної безпеки компанії.

A method of managing complex state of protection of information security by analyzing the causal relationships by Ishikawa method to improve the quality of information security management of the company. Adequate assessment of information risk and optimizing investments in information security approaches and procedures are applied, based on existing international standards for risk management of information security. Unfortunately, these standards are mostly conceptual and advisory in nature and doesn't take into account many factors that significantly affect the accuracy and objectivity of the risk assessment. The method of determining the complex state of security by analyzing the causal relationships by Ishikawa method makes it possible to consider as the attacker factors of danger and protective factors of the company, as well as by the economic-cost approach to risk analysis, provide information on the costs and investments in information security. The proposed method uses socio-psychological and motivational performance figures of the attacker, technical parameters of the facilities, business information and financial capabilities of the company, allowing for a comprehensive assessment. This method allows you to combine both the minimum and the required number of parameters to optimize research of information and financial risks. The proposed method through simple scalability covers all the necessary parameters for a comprehensive assessment of the security of information security company.

Ключові слова: Інформаційна безпека, метод визначення загального стану захищеності, комплексна оцінка інформаційних ризиків, інформаційна безпека компанії, метод Ісікави, діаграма "риб'ячої кістки".
Key words: Information Security, the method of determining the complex state of information security, complex assessment of information risks, information security company, the method of Ishikawa "fish bone" diagram.

ВСТУП

Проблема оцінювання та дослідження інформаційних ризиків асоціюється з багатьма провідними методами [1], які широко використовуються на сьогоднішній день та які відповідають багатьом міжнародним стандартам [2], але не враховують додаткових факторів. Дані методи виконують функцію обмеження проведення оцінки відповідно до сучасних нормативно-правових рекомендацій для урегулюван-

Таблиця 1. Мінімально необхідний набір даних для визначення загального стану захищеності компанії

Зловмисник-співробітник (W):	**Об'єкт (O):**
Об'єм додаткових ресурсів (m) Мотивацію зловмисника (y) Соціально-психологічний тип зловмисника(Ph) Доступи до об'єктів Атаки на обє'кти (A1 .. An)	Атаки на об'єкт (A1 .. An) Об'єм інформації в об'єкті (V) Показник технічної захищеності об'єкта (KT) Доступи зловмисників до об'єкту
Атаки (A):	**Компанія (CC):**
Витрати на реалізацію атаки (D) Виграш від реалізації атаки (g) Неочікувані витрати на реалізацію атаки (d) Показник ймовірності реалізації атаки (Pt)	Коефіцієнт стабільності компанії по реєстраційній групі (CCR) Коефіцієнт стабільності компанії по управлінській групі (CCM) Критичну вартість приватних ресурсів компанії (qp) Критичну вартість соціальних ресурсів (qs) Ринкову вартість інформації компанії (R)

ня визначення рівня інформаційної безпеки на основі наданої інформації замовником, або отриманої інформації в процесі аудиту компанії. В основному серед інформації, яка розглядається при оцінці інформаційних ризиків фігурують нормуючі показники: інвестиції в інформаційну безпеку, витрати на реалізацію комплексу захисту, витрати на реалізацію загрози та можливі втрати, що в свою чергу є достатньо обмежуючим факторами при проведенні оцінки.

Комплексна оцінка інформаційних ризиків у наш час вимагає врахування багатьох параметрів, серед яких визначається чотири основні: соціально-психологічні показники особистості зловмисника, технічний рівень захисту компанії або об'єкта, ймовірність реалізації конкретної загрози конкретним зловмисником і, звичайно, показник стабільності компанії. Це далеко не всі показники, які можуть бути присутні в процесі оцінки інформаційних та фінансових ризиків компанії, але вищезазначені є основою для проведення коректної оцінки, а також на них звертають найбільшу увагу при формуванні систем захисту.

Використання чотирьох приведених показників дає можливість отримати інформацію про компанію, яка покриває всі можливі джерела виникнення загроз та при використанні даних показників для комплексної оцінки компанії, це дає можливість отримати інформацію по кожному з об'єктів, що захищаються, співробітників, які можуть бути як зловмисниками, так і предметом атаки, можливих зовнішніх зловмисниках або принаймі уявлення про тип зовнішнішнього зловмисника, загрози, що відображають недоліки, що можуть перетворитися у втрати.

Для того, щоб отримати комплексну оцінку інформаційних ризиків при проведені аудиту компанії в нашому досліджені запропоновано використати метод аналізу причинно-наслідкових взаємозв'язків за Ісікавою [3], який є одним із семи основних методів оцінки та контролю покращення якості виробничих процесів.

ВИЗНАЧЕННЯ ЗАГАЛЬНОГО СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ НА ОСНОВІ БАГАТОФАКТОРНОГО АНАЛІЗУ КОМПАНІЇ

Загальний стан інформаційної безпеки об'єкта або загальний стан захищеності компанії визначається за допомогою чотирьох основних факторів, які задовольняють обмежуючому правилу управлінського стандарту при побудові діаграми Ісікави [3]:

$$Z(t) = CC + W + O + A + X \qquad (1),$$

де CC — фактор (причина) стабільності компанії, W — фактор (причина) небезпеки зловмисника(-ів), O — фактор (причина) ймовірності реалізації атаки виходячи з захищеності об'єкту, через який реалізується загроза або показник технічної захищеності об'єкта, A — фактор (причина) ймовірності реалізації конкретної атаки конкретним зловмисником, що входять у вираз для обчислення загального стану захищеності, X — невідомий фактор, який впливає на наслідок, але є невідомим в момент проведення аналізу. Загальний стан захищеності — це діапазон значень Z(t)=[z0:zn], який включає всі можливі сценарії розвитку реалізації загроз по кожному з об'єктів з використанням всіх можливих атак по об'єкту, а також всіх співробітників. Тобто, загальний стан захищеності, це повний перебір всіх можливих атак по всіх можливих каналах та через всі об'єкти. Якщо ж загальний стан захищеності потрібно визначити для конкретного обє'кту, атаки чи співробіника, які впливають на зміну факторів відносно об'єкта, атаки чи співробітника, то в такому випадку формула 1 універсальна в своєму застосуванні як для комплексної оцінки, так і для оцінки конкретних випадків.

Для проведення оцінки загального стану захищеності компанії або об'єкта експертам з інформаційної безпеки потрібно отримати дані про компанію. На сьогодні найбільш поширеним методом отримання актуальних даних про компанію є аудит компанії. Аудит може бути внутрішнім або зовнішнім, так і спеціально проведеним експертами з інформаційної безпеки. Результатом проведеного аудиту повинен бути мінімально-необхідний набір даних, які потрібні для аналізу та визначення загального стану захищеності компанії. Мінімально необхідний набір даних потрібний для оцінки приведений в таблиці 1. Фактично дані в таблиці 1 є двома першими кроками в побудові діаграми Ісікави, а саме виявленням й збором всіх факторів і причин, що впливають на досліджуваний результат, а в нашому випадку це загальний стан захищеності компанії, та групування факторів по рівню впливу і причинно-наслідкових блоках.

На основі представлених даних побудуємо діаграму Ісікави та проставимо частки для кожного з факторів на основі експертної оцінки, яку отримано шляхом проведення оцінок інформаційної безпеки підприємств за допомогою використання економіко-вартісних моделей [4]. В реальній практиці проведення оцінки загального стану захищеності компанії для визначення часток факторів (причин) потрібно використовувати комбінований метод експертних оцінок або один з критеріальних методів оцінки.

На рисунку 1 представлена дворівнева діаграма Ісікави, на першому рівні позначені головні фактори, які впливають на загальний стан захищеності компанії, а на другомі рівні показано деталізацію факторів, тобто фактори другого рівня. На першому рівні додається ще один фактор X, який за Ісікавою залишається порожнім, бо невідомо чи всі фактори враховані при виявлені можливих факторів впливу. Загалом прийнято деталізовувати до пятого рівня, але в нашому досліджені обмежуємося двома рівнями. Слід зауважити, що в представленому випадку на діаграмі Ісікави не представлено факторів першого рівня, які впливаються на зменшення негативного впливу на загальний стан захищеності компанії. Що стосується першого рівня, то єдиним фактором впливу на покращення загального стану захищеності інформаційної безпеки компанії є інвестиції в заходи та засоби забезпечення інформаційної безпеки підприємства, серед таких заходів можуть бути, як і впровадження певних нормативно-правових рекомендацій, так і закупка обладнання і т.д. Впровадження всіх заходів та засобів всеодно відображаються в фінансовому еквіваленті. Якщо розглянути в розрізі чотири представлених фактори, то покращення стану безпеки за рахунок інвестицій загалом розшиваються на чотири фактори представлені на першому рівні, це означає що проінвестувавши допустимо в технічний захист об'єкту закупивши нове обладнання, отримуємо позитивний вектор для фактора Об'єкт на другому рівні, розглянувши по всіх решту факторів, отримуємо, що фактор інвестиція першого рівня втрачає свою суть на першому рівні та при аналізі виявлено доцільніше за рахунок декомпозиції розміщати його по факторах другого рівня, що дозволить більш детально розглядати позитивний вплив на конкретний фактор. Також слід зазначити, що на діаграмі пропущені та невідображені зв'язки зловмисник — атака — обєкт, які характеризують, який зловмисник, яку атаку може провести і на який обєкт, бо ці зв'язки відображають, як зв'язані різні фактори між собою і не впливають на причино-наслідковий аналіз факторів, але при визначені

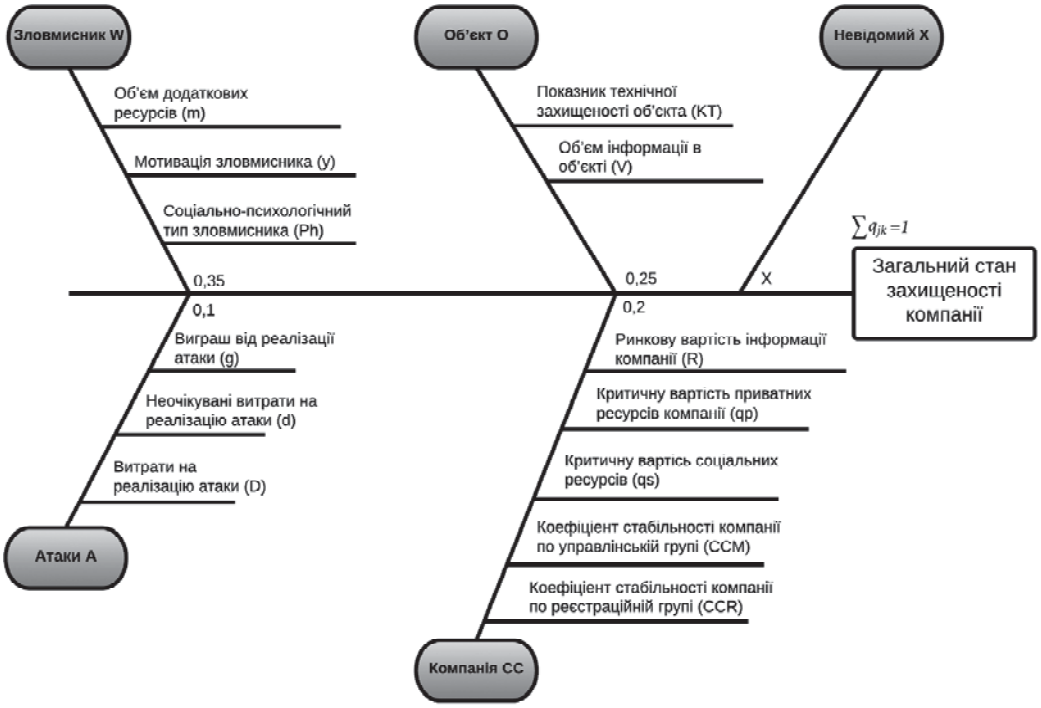

Рис. 1. Діаграма Ісікави для управління загальним станом захищеності компанії

загального стану вони використовують сповна для відображення повних маршрутів атак і побудови карти атак. Загальний стан інформаційної безпеки компанії виходячи з управлінського стандарту Ісікави називається розбалансуванням відносно ідеального стану системи. Проектуючи ідеальний стан системи на інформаційну безпеку отримуємо, що це такий стан системи, коли захищені та невразливі абсолютно усі активи. Отже, результатом причино-наслідково аналізу комплексного захисту компанії є розбалансування, стан системи та інформація про те на який фактор потрібно впливати, щоб старатися досягнути ідеального стану захищеності системи. Розглядаючи обмеження ідеального стану та результати розбалансування. Потрібно звернути увагу на 5 обмежуючих правил [5].

У дослідженнях для широко- та вузькопрофільних компаній щодо інформаційної безпеки пропонується відходити від оцінки інформаційної безпеки компанії по чотирьох запропонованих показниках, але використовуючий метод концептуально в оцінці загального стану компанії нічого не поміняється. В випадку розширення факторів, за якими проводиться оцінка загального стану захищеності компанії, отримаємо просто більшу вибірку загальних станів захищеності, яка збільшуватиметься пропорційно кількості факторів, які використовуються для оцінки загального стану захищеності. Якщо ж для управління буде використовуватися метод Ісікави, то в такому випадку передбачається, що, коли невідомі всі фактори або фактори можуть змінюватися, залишається одна додаткова причина, для якої проставляють відповідну частку в процесі аналізу.

Використання економіко-вартісних моделей при рохрахунку розбалансування за допомогою аналізу причинно-наслідкових взаємозв'язків за методом Ісікави.

Для того, щоб провести оцінку загального стану захищеності та використати для визначення загального стану захищеності формулу (1), потрібно провести деякі додаткові розрахунки показників. Для визначення стабільності компанії по реєстраційній групі CCR проводиться адитивна звертка на основі типових параметрів компанії визначених за допомогою аудиту, ці дані є у відкритому доступі та не потребують додаткових запитів. Дані, що використовуються для обчислення показника стійкості компанії реєстраційній групі CCR: ccr1 — мета і характер діяльності, ccr2 — форма власності, ccr3 — належність капіталу, ccr4 — правовий статус і форма господарювання ccr5 — галузево-функціональний вид діяльності, ccr6 — технологічна і територіальна цілісність, ccr7 — розмір середньооблікового за чисельністю працівників і сумою валового доходу від реалізації продукції, де кожен з показників має свій кількісний показник. Показник стійкості компанії по реєстраційній групі обчислюється за формулою (2):

$$CCR = a1 * ccr1 + a2 * ccr2 + \cdots + a7 * ccr7 \quad (2).$$

Дані, що використовуються для обчислення показника стійкості компанії по управлінській групі CCM: ccm1 — фінансовий стан компанії, ccm2 — взаємовідносини з клієнтами, ccm3 — внутрішні бізнес процеси, ccm4 — навчання і збільшення кваліфікації працівників. Показник стійкості компанії по реєстраційній групі обчислюється за формулою (3):

$$CCM = b1 * ccm1 + b2 * ccm2 + b3 * ccm3 + a4 * ccr4 \quad (3).$$

Для покращення оцінки стійкості компанії можна вводити додаткові показники, але їх введення потрібно обгрунтовувати наявністю у всіх компаній, котрі працюють на ринку. Запропоновані показники CCR підтверджуються законодавством України та підходять для компаній, які працюють, як офіційно так і в тіні, що дозволяє проводити оцінку інформаційних ризиків у таких компаніях без проблем та не потребує розробляти для таких компаній окремого методу оцінки, а показники CCM є даними, які постійно регуляно використовуються при управлінні змінами провідними експертами.

Для визначення соціально-психологічного типу зловмисника Ph, показник визначає можливі поведінкові особливості кожної особистості та нестандартні реакції прояву, в результаті застосування методики [6] для оцінки соціально-психологічного типу зловмисника отримаємо тип зловмисника інформаційної безпеки та коефіцієнт небезпеки зловмисника Ph. Для визначення типу зловмисника використовуються типи зловмисника інформаційної безпеки на основі соціально-психологічних типів особистості, для кожного зловмисника визначається його соціально-психологічний тип та конвертується в кількісну оцінку небезпеки типу зловмисника Ph. Для зловмисників всіх типів: інстайдерів, аустайдерів та інсайдерів-аутсайдерів, об'єм додаткових ресурсів M визначається як співвідношення (4) між його наявними ресурсами m і прямими D та неочікуваними d витратами на реалізацію конкретної загрози [7]:

$$M = \frac{m}{D + d} \quad (4).$$

Слід зазначити, що неочікувані витрати зловмисника на проведення протиправних дій можуть бути надзвичайно малими $d \to 0$, якщо зловмисник зміг детально все прорахувати, а також можуть бути нескінченно великими $d \to \infty$, якщо зловмисник халатно підготувався до проведення протиправних дій і не врахував різні фактори небезпеки. Ще одним параметром для визначення показника небезпеки зловмисника є його мотивація y, що визначається за наступним співвідношенням (5):

$$y = \frac{g(t)}{g^A} = \frac{g^1}{g^{SC}} \quad (5),$$

де g(t) — виграш зловмисника від реалізації викраденої інформації в певний момент часу, g^A — середній виграш зловмисника за оцінкою компанії, g^{SC} — критична вартість викрадених приватних та соціальних ресурсів, що визначається як $g^{SC} = g^P + g^S$. Отож, показник небезпеки конкретного зловмисника W визначається за формулою (6):

$$W = Ph * M^*y \quad (6).$$

Набір можливих атак A1..An визначаються з аналізу типу об'єкта та каналів доступу до об'єкта в інфраструктурі компанії. Також для кожного обсягу з результатів аудиту визначається частина обсягу інформації V в об'єкті від загальної інформації в компанії в % або ж в умовних одиницях, які після визначення ринкової вартості інформації R, можуть бути перераховані в фінансовий еквівалент. Показник технічної захищеності обєкта О визначається на основі аналізу його захищеності по кожній з атак, тобто об'єкт отримує у відповідність кожній атаці значення його захищеності, яке визначається в межах від 0 до 1 в залежності від критичної вразливості від проведення цієї атаки. Для визначення показника ймовірності реалізації конкретної атаки А, для кожної атаки проведеної конкретним співробітником на конкретний об'єкт використовуємо економіко-вартісну модель [7; 8], застосування цієї моделі дозволяє виключити з розрахунків атаки, які неможливі для реалізації на момент проведення аудиту за відсутності необхідних навиків в співробітника, а також відсутності необхідних ресурсів, тобто в кінцеву вибірку попадають тільки ті атаки, які дійсно може провести співробітник. Розрахунок проводитися за формулою (7):

$$A = 1 - \frac{(D+d)}{g} = 1 - \frac{(D+d)}{VR} \quad (7).$$

Розглянувши обчислення всіх показників, отримуємо можливість провести обчислення загального стану захищеності компанії через кожну атаку по конкретному об'єкту конкретним співробітником за формулою 1. Результати оцінки загального стану захищеності компанії, об'єкта або конкретного співробіника в подальшому необхідні для визначення інвестицій в інформаційну безпеку та ефективності цих інвестицій. В попередніх дослідженнях, нема чіткого визначення загального стану захищеності компанії, а є лише рекомендації, щодо витрат або ж інвестицій в інформаційну безпеку, які не повинні перевищувати 37% від загального обсягу інвестицій або витрат компанії на управління інформаційною безпекою, тому на цьому було хибно сформоване уявлення про загальний стан захищеності. Поправка дослідження [9] призвело до того, що число з 37% виросло до 52,48% і теж є не коретним, тому що оцінка привязана до визначеної функції, яка на думку авторів є "оптимальним варіантом" при визначенні розподілу інвестицій і дана функція не відображає реального стану захищеності або інформаційних ризиків компанії. Завдяки застосуванні параметрів $Z(t)$ інвестиції в інформаціну безпеку зможуть бути визначенні на більш точному рівні та розподілені коректно між обєктами атаками та співробітниками-зловмисниками завдяки використання наслідкових взаємозв'язків та економіко-вартісних моделей, які в свою чергу використовують реальні дані аудиту компанії.

ВИСНОВКИ

Найбільш поширеним у практиці захисту інформації методам аналізу та дослідження ризиків, наведеним у міжнародних та національних стандартах, властивий ряд вад, зокрема, занадто загальний концептуально-рекомендаційний характер подання матеріалів, що практично виключає можливість врахування при аналізі характерних специфічних властивостей об'єктів ризику й істотно зменшує об'єктивність та точність отриманих результатів. Крім того, орієнтація нових стандартів з інформаційної безпеки серії ISO 27000 на ітеративну процедуру управління ризиками за Шухартом-Демінгом обумовлює застосування переважно перебірного підходу у побудові СЗІ, звужуючи можливості застосування аналітичних оптимізаційних методів.

З іншого боку, використання відомих моделей Гордона-Лоеба для дослідження проблеми ефективності інвестування у системи захисту практично виключає можливість врахування у цих дослідженнях конкретики реального об'єкту ризику й фактично відмежовує цей підхід від прикладних досліджень реальних об'єктів ризиків. Загалом модель Гордона-Лоеба не пристосована для розв'язання прикладних вузькопрофільних задач

У цій ситуації перспективним видається застосування для аналізу загального стану захищеності компанії метод аналізу причинно-наслідкових взаємозв'язків, що базується на аналізі відомих факторів, які уже "працюють" в компаніїї і відомі учасникам оцінки, а також рекомендації щодо мінімального набору даних, які потрібні для повноти оцінки інформаційної безпеки. Для тощо, щоб результати аналізу набули кількісних значень пропонується використовувати економіко-вартісні моделі, які зарекомендували себе при проведені оцінки інформаційної безпеки. Використовуючи комбінацію методу причинно-наслідкових взаємозв'язків та економіко-вартісних моделей дає не тільки можливість управляти інформаційною безпекою на управлінському рівні, але і дає можливіть приймати конкретні рішення завдяки отриманні реальних оцінок виходячи з реальних даних про компанію.

Література:

1. ISO/IEC 27005 — Information security risk management/
2. BS 31100:2011 Risk management. Code of practice and guidance for the implementation of BS ISO 31000/
3. Ishikawa K. Guide to Quality Control. — Tokyo, Asian Productivity Organization, 1976.
4. Архипов О.Є., Скиба А.В., Хоріна О.І. Розширення економіко-вартісних моделей інформаційних ризиків за рахунок використання соціально-психологічних типів зловмисника // Захист інформації 17 (1). — Київ. — 2015. — С. 60—72.
5. Ishikawa K. What is Total Quality Control The Japanese Way. London, Prentice Hall, 1985.
6. Скиба А., Хоріна О.І. Прогнозування соціально-психологічних та ситуаційних чинників активації злочинних думок і намірів у сфері інформаційної безпеки. // Безпека інформації — 2015. — Т. 21, № 2. — С. 165—173.
7. Архипов О.Є., Скиба А.В. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації (стаття) // Захист інформації. — 2012. — Т. 15, № 4. — С. 366—375.
8. Arhupov O., Skyba A. Methods and Approaches to Investigating Information Risks by Means of Economic Cost Models // The Advanced Science Journal. — Vol. 12. — С. 75—82.
9. Gordon L.A., Loeb M.P., Lucyshyn W., & Zhou L. "Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model" // Journal of Information (2014) Security. — Vol. 6.

References:

1. ISO/IEC 27005 (2011), "Information security risk management", available at: http://www.iso27001security.com/html/27005.html (Accessed 20 Nov 2015).
2. BSI (2011), "BS 31100:2011 Risk management. Code of practice and guidance for the implementation of BS ISO 31000", available at: http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030228064&industry=risk (Accessed 20 Nov 2015).
3. Ishikawa, K. (1976), Guide to Quality Control, Asian Productivity Organization, Tokyo, Japane.
4. Arkhypov, O. Skyba, A. and Khorina, O. (2015), "An extension of economic cost model of information risks indentification by social-psychological types of attacker", Information Security Research Journal, vol. 17, № 1, pp. 60—72.
5. Ishikawa, K. (1985), What is Total Quality Control The Japanese Way, Prentice Hall, London, UK.
6. Skyba, A. and Khorina, O. (2015), "Expanding of economic-cost models for risk evaluation of information security by the typology of personality by H. Eysenck", Ukrainian Scientific Journal of Information Security, vol. 21, no. 2, pp. 165—173.
7. Arkhypov, O. and Skyba, A. (2012), "Information risk: research methods and techniques, models and methods of risk identification", Information Security Research Journal, vol. 15, no. 4, pp. 366—375.
8. Arhupov, O. and Skyba, A. (2014), "Methods and Approaches to Investigating Information Risks by Means of Economic Cost Models." The Advanced Science Journal, vol. 12, pp. 75—82.
9. Gordon, L. A. Loeb, M. P. Lucyshyn, W. and Zhou, L. (2014), "Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model", Journal of Information Security, vol. 6.

Стаття надійшла до редакції 25.12.2015 р.