УДК 681.3.06

АНАЛІЗ СИСТЕМ ПОКАЗНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ

О.В. ПОТІЙ, Д.Ю. ПИЛИПЕНКО

В роботі проаналізовано існуючі на сьогоднішній день системи показників безпеки інформації. Дані системи або таксономії розглянуто як інструмент, здатний надати можливість комплексно охарактеризувати стан безпеки інформації підприємства. Розглядаючи таксономії показників безпеки інформації у такому контексті, були визначені їхні головні властивості, переваги та недоліки.

Ключові слова: показник безпеки інформації, програма забезпечення безпеки інформації, таксономія показників.

ВСТУП

Сьогодні можна із впевненістю говорити, що у галузі інформаційної безпеки (ІБ) особа, що приймає рішення (ЛПР) вже не може спиратися лише на інтуїцію. Прийняттю більш обґрунтованих рішень можуть сприяти показники безпеки, користуючись якими ЛПР отримає можливість приймати рішення, вважаючи умови динамічного мінливого середовища.

На прийняття рішень впливають фактори: суб'єктивні (досвід ЛПР, що є результатом прийнятих у минулому рішень та отриманих наслідків, знання ЛПР у цій галузі, інтуїція) та об'єктивних (різного роду показники). Перша група факторів в значній мірі залежать від особистості ЛПР, і вплинути на них важко. Проте, за допомогою об'єктивних показників безпеки інформації можна сформувати інформаційну повноту, спираючись на яку ЛПР зможе прийняти більш обґрунтоване рішення.

У 2001 р. пройшла перша конференція, що була повністю присвячена питанням оцінювання інформаційної безпеки, – Workshop on Information, Security System Scoring and Rankin. В матеріалах даної конференції [1] містяться ключові погляди фахівців у галузі інформаційної безпеки, обговорюється безліч проблем, пов'язаних з оцінюванням інформаційної безпеки. З цього моменту в англомовній літературі починає активно вживатись термін «security metrics», який на українську мову можна перекласти як метрика безпеки або – більш коректно – показник безпеки. Необхідно зауважити, що через різні переклади використовуються різні поняття, і тлумачення самих понять також не завжди співпадає. Це призводить до певної плутанини у термінах, тому на даний момент існує потреба в єдиній затвердженій терміносистеми у напрямку оцінювання безпеки інформації.

1. ТАКСОНОМІЯ ПОКАЗНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ VAUGH–HENNIG–SIRAJ

В роботі [2] підбиваються підсумки конференції WISSRR [1] та обговорюються ключові проблеми, що з'явилися під час проведення досліджень у цьому напрямку. Автори запропонували та обґрунтували свою версію таксономії показників безпеки. Ефективність набору показників безпеки з точки зору авторів залежить від цілої низки факторів: поставлених задач безпеки; технічних, організаційних та операційних потреб; доступних фінансових, кадрових та технічних ресурсів.

Під час створення цієї системи показників безпеки автори в деякій мірі користувалися спостереженнями Дебори Бодо [2], якою було запропоновано розглядати показники як векторний добуток об'єкта вимірювань, мети вимірювань та особи, для якої призначені результати вимірювань. Рис 1. ілюструє цю концепцію:

Різноманіття підприємств, діяльність яких відбувається у своєму специфічному середовищі, дійсно створює ситуацію, коли одним набором показників неможливо задовольнити усі потреби. На вибір показників безпеки інформації неминуче впливає розмір підприємства, доступні ресурси та рівень зрілості процесів підприємства.

Інформаційна безпека з точки зору авторів становить поєднання трьох елементів, а саме *тех-*

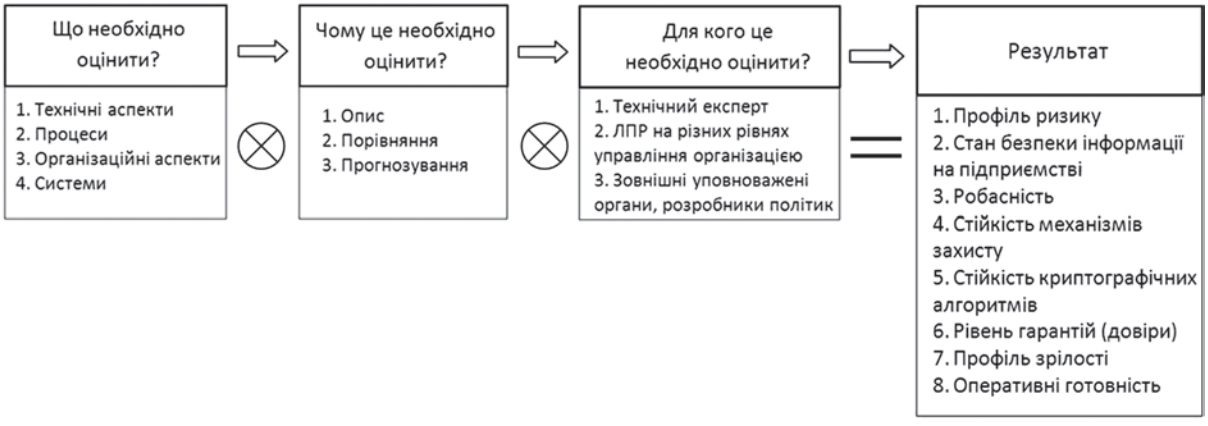

Рис. 1. Модель показника безпеки інформації Бодо

нології, що обумовлює захист, *процесу*, в котрому ця технологія використовується, та *людей*, завдяки яким ця технологія працює. Розвиваючи цю ідею, можна припустити, що показники безпеки інформації повинні охоплювати усі три елемента – продукт, процес та кадри.

Було запропоновано поділити усі показники безпеки на дві категорії: *організаційні показники безпеки* та *показники оцінювання технічних об'єктів* (рис. 2). Організаційні показники використовуються для оцінювання ефективності/результативності програми забезпечення безпеки інформації (програма ЗБІ) та процесів захисту інформації, впроваджених на підприємстві. За допомогою цих показників формується зворотній зв'язок у циклі управління та вдосконалення діяльності з забезпечення безпеки інформації. Клас показників оцінки технічних об'єктів впроваджено для оцінювання того, наскільки добре технічні об'єкти (продукти, системи, засоби захисту тощо) здатні забезпечити довіру (гарантії) у термінах захисту від атак, їх виявлення та реагування на інциденти безпеки.

Ключовою особливістю даної роботи є вперше запропонована цілісна таксономія показників безпеки інформації. Ця таксономія поєднує різні групи показників та дозволяє охарактеризувати діяльність підприємства у контексті забезпечення безпеки інформації. Проте, авторами не було запропоновано конкретних показників. Рішення цієї задачі було покладено безпосередньо на фахівців, що будуть адаптувати запропоновану таксономію до конкретних специфічних умов свого підприємства.

2. ТАКСОНОМІЯ ПОКАЗНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ OCTAVE

У 2001-2003 роках інститутом SEI було розроблено метод OCTAVE (Operational Critical Threat, Asset and Vulnerability Evaluation), що дозволяє підприємству ідентифікувати ризики для своїх найбільш важливих інформаційних активів та розробити стратегічній план усунення виявлених ризиків безпеки [3]. В рамках цього методу виділяється етап оцінювання поточного стану діяльності з захисту інформації. Для рішення цієї задачі було розроблено каталог практик безпеки та спеціальну анкету, які, по суті, являють собою засіб оцінювання поточної практики безпеки на підприємстві та формування відповідної стратегії покращення практичної діяльності для забезпечення більш ефективного захисту критичних активів. На рис. 3 наведено таксономію показників безпеки інформації, розроблену згідно з каталогом практик безпеки OCTAVE [3]. Декомпозиція показників обґрунтовується тим, що метод OCTAVE, насамперед, орієнтовано на рішення проблем безпеки, пов'язаних не з технологіями, а з практичною діяльністю. Цей метод працює у площині операційних ризиків безпеки та практики безпеки інформації, а технологія розглядається тільки по відношенню до практики безпеки. Розробники каталогу практик безпеки спиралися на декілька джерел, головним чином на нормативні документи [4, 5], а також на власні розробки інституту SEI.

Отже, всю множину показників безпеки було поділено на два класи: показники стратегічної та операційної діяльності із забезпечення безпеки інформації. Вони складають перший рівень ієрархії.

Показники стратегічної діяльності, насамперед, орієнтовані на оцінювання організаційних проблем на рівні політик безпеки інформації та корпоративного управління безпекою. Стратегічна діяльність пов'язана із загальними бізнесцілями підприємства та потребує наявності корпоративних планів та участі вищого керівництва у вирішенні цих проблем. Показники операційної діяльності використовуються для оцінювання проблем, пов'язаних здебільшого з використанням технологій захисту у повсякденній діяльності співробітників підприємства.

Рис. 2. Таксономія показників безпеки інформації Vaugh–Hennig–Siraj

На другому рівні ієрархії вводяться підкласи стратегічних показників (6 підкласів) та операційних показників (3 підкласи), які в свою чергу також розкладаються на підкласи. У кожному підкласі другого рівня стратегічних показників і третього рівня операційних показників визначаються декілька чинників, що підлягають оцінюванню. Наприклад, у класі стратегічних показників оцінювання стратегії захисту виділяються показники, що характеризують:

• облік бізнес-стратегій під час розглядання питань з безпеки інформації;

• облік стратегії безпеки у загальних стратегічних цілях та задачах підприємства;

• якість та періодичність перегляду та оновлення документації, від ображаючої стратегію безпеки, цілі та задачі захисту.

У класі операційних показників криптографічного захисту вводяться показники, що характеризують:

• застосування засобів криптографічного захисту інформаційних активів;

• застосування криптографічних протоколів під час передачі інформації, реалізації віддаленого доступу до ресурсів;

• періодичність аналізу, верифікації та модифікації криптографічних засобів захисту інформації та протоколів.

Оцінювання є якісним та здійснюється методом експертного опиту та аналізу стану практики інформаційної безпеки на підприємстві. Таксономія OCTAVE складається з показників якісного типу. Наведена методика не надає чітких інструкцій відповідно того, яким чином необхідно організовувати процес моніторингу ризиків.

3. ТАКСОНОМІЯ ПОКАЗНИКІВ БЕЗПЕКИ ОСІРЕР

Цю таксономію було розроблено у 2004 р. групою канадських фахівців для уряду Канади (Департамент захисту критичної інфраструктури та надзвичайних ситуацій) [6]. Під час розробки цієї таксономії автори дотримувалися ширших поглядів щодо оцінювання безпеки інформації. Вони висловлюють наступну ідею: оцінювання безпеки інформації повинно формуватися у рамках *концепції інформаційної довіри* чи *інформаційних гарантій* (Information Assurance, IA), або *гарантій інформаційної інфраструктури* (Information Infrastructure Assurance). Під цим терміном автори розуміють здатність мереж та систем забезпечити своєчасну передачу інформації між двома або більше сторонами із заданою точністю та безпекою. Інформаційна довіра складається з трьох базових елементів: забезпечення безпеки інформації (Security Information), забезпечення якості послуг (Quality of Service, QoS) та доступність IT-інфраструктури (Availability). Спираючись на приведене визначення IA та три ключових елементи інформаційної довіри, автори пропонують свій варіант таксономії. При цьому основним об'єктом оцінювання стають системи інформаційних технологій та мереж.

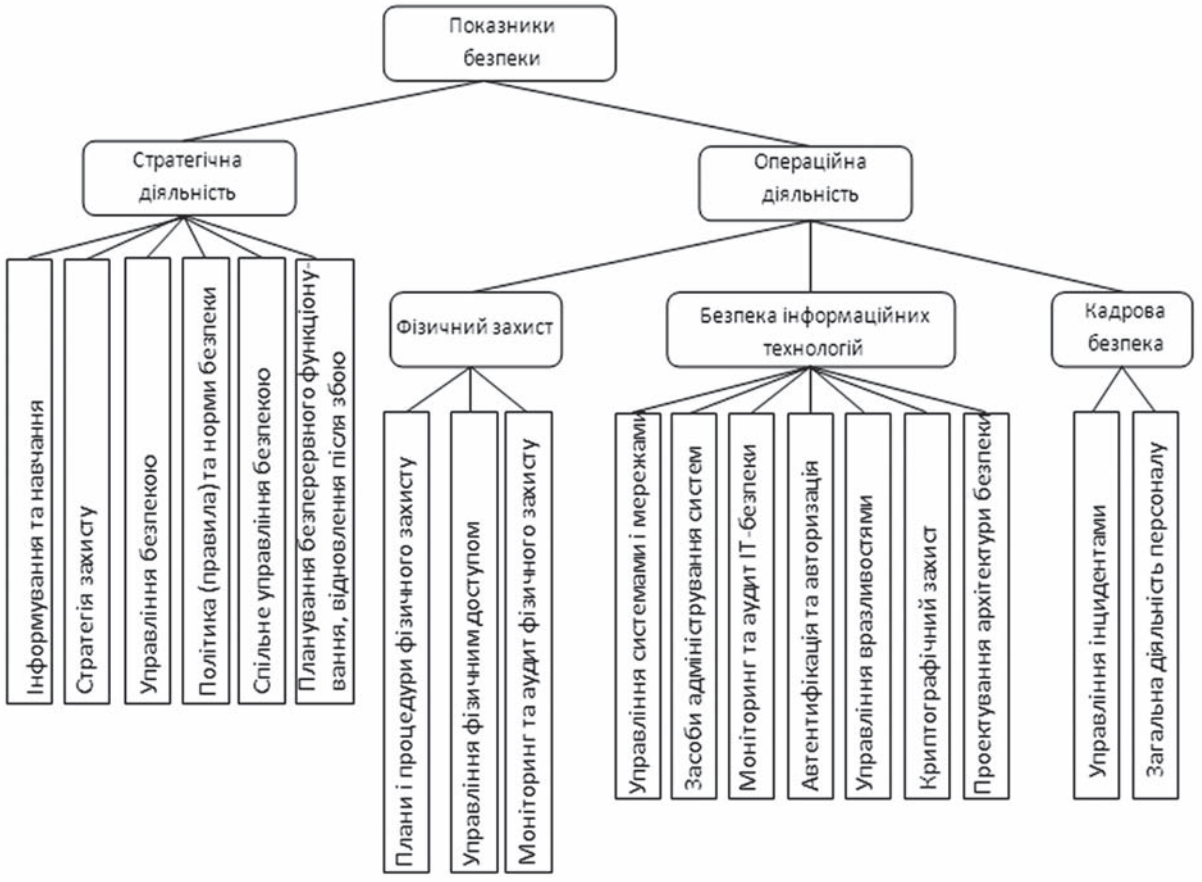

Рис. 3. Таксономія показників безпеки інформації OCTAVE

Таксономія показників OCIPEP є багаторівневою (рис. 4). Перший рівень ієрархії формується по ключовим елементам ІА. Другий рівень ієрархії формується таким само чином, як і в таксономіях WISSRR, Vaugh–Hennig–Siraj та NIST, тобто вся множина показників поділяється на показники організаційного управління, показники оцінювання операційної практики захисту інформації та показники оцінювання технічних елементів.

Далі відбувається більш детальна декомпозиція показників у кожному класі. Група показників організаційного управління використовується для оцінювання того, яка увага приділяється питанням забезпечення безпеки інформації. До цієї групи належать показники, що характеризують такі аспекти, як розробка програми ЗБІ (оцінювання якості планування захисту, управління ризиками безпеки, розробка політики безпеки) та управління ресурсами (кадрове забезпечення та матеріально-технічне забезпечення захисту інформації).

Група операційних показників характеризує підприємство з точки зору досягнення цілей безпеки, виконання політики безпеки та вирішування задач захисту. Ця група складається з показників технічної готовності (якість документування, цілісність даних, якість планування безперервного функціонування), оцінювання вразливостей мережі у конкретному середовищі безпеки, ефективність діяльності із захисту інформації.

Група показників оцінювання технічних елементів використовується для оцінювання того, наскільки вимоги безпеки інформації забезпечуються технічними компонентами мережі. До цієї групи належать статистичні показники оцінювання засобів захисту інформації (програмних, апаратних, програмно-апаратних засобів), статистичні показники інцидент інцидентів безпеки у мережі (системі), динамічні показники тестування безпеки (тестування на проникання, тестування на відмову в обслуговуванні).

Під час розробки таксономії показників OCIPEP автори спирались на таксономії NIST, WISSSR та Vaughn–Hennig–Siraj, розглядаючи можливість сформувати з них фундамент для таксономії, яку можна використовувати для оцінювання комп'ютерних мереж. Автори дійшли наступних висновків: наведені таксономії не можуть бути застосовані для оцінювання стану комп'ютерної мережі по трьом факторам, а саме захищеності, доступності та QoS. Таким чином, авторами було запропоновано нову таксономію та категорію показників, за допомогою яких можна отримати оцінювання інформаційних гарантій для комп'ютерної мережі. Слід зауважити, що в рамках таксономії OCIPEP не було запропоновано конкретних показників та методології проведення вимірювань.

4. ТАКСОНОМІЯ ПОКАЗНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ CISWG

В 2004 році робочою групою корпоративної інформаційної безпеки (Corporate Information Security Working Group, CISWG) підкомітету технологій, інформаційної політики та міжурядових взаємодій уряду США було підготовлено звіт, що містив рекомендації щодо найкращих практик безпеки (діяльність із захисту інформації). Наведені рекомендації інтерпретувались як складові елементи програми ЗБІ, а також у якості підтримки до них було запропоновано кількісні показники безпеки інформації [7]. Запропонована система практик може бути використана будь-якими підприємствами (державними, академічними, комерційними) для розробки програми ЗБІ або удосконалення вже існуючої. Автори підкреслюють, що основною їхньою задачею була розробка ресурсу, користуючись яким, керівництво, менеджери та технічний персонал отримає можливість розробити свій комплекс принципів, політик, процесів, засобів захисту та показників продуктивності, спрямованих на співробітників, процеси та технологічні аспекти інформаційної безпеки.

Автори акцентують увагу на тому, що відправним пунктом в формуванні програми ЗБІ є запропонований керівництвом набір принципів, на базі якого і буде сформовано комплекс заходів, що складається з політики безпеки, процесів, заходів із забезпечення безпеки інформації та показників продуктивності. Даний момент вартий уваги з приводу того, що автори пропонують спадний підхід до формування програми ЗБІ. Ідея включення у цей процес також і вищого керівництва, безперечно, корисна, оскільки подібна взаємодія керівництва та співробітників, що безпосередньо зайняті організацією безпеки інформації, сприятиме узгодженню бізнес-цілей підприємства та цілей ІБ.

Запропонована таксономія показників дозволяє будь-якому підприємству розробити свою систему показників для оцінки ефективності ре-

Рис. 4. Загальна таксономія показників безпеки інформації OCIPEP

алізації програми ЗБІ. Показники демонструють те, наскільки ефективно здійснюються політики безпеки, процеси та заходи захисту інформації, чи досягаються поставлені цілі безпеки. Наведені у цій роботі показники вимірюють стан або ефективність реалізації заходів захисту інформації, проте не стосуються пов'язаних з цим ризиків. Управління ризиками потребує додаткових робіт, які складаються з виявлення ймовірності реалізації загроз, виявлення вразливостей та можливих збитків.

Показники безпеки дозволяють здійснювати безперервне покращення процесів, сприяють зростанню рівня зрілості процесів, оскільки вони надають об'єктивний спосіб оцінювання стану певного об'єкту інформаційної безпеки. На рис. 5 наведена таксономія показників безпеки, розроблена на базі елементів загальної програми ЗБІ CISWG.

Таксономія CISWG налічує 99 показників безпеки інформації. Уся множина показників поділена на три групи: показники підтримки стратегічної практики управління безпекою (7 напрямків діяльності та 12 показників), показники підтримки оперативного управління (10 напрямків та 42 показники безпеки) та показники підтримки технічної діяльності із захисту інформації (13 напрямків та 45 показників безпеки інформації). Робоча група виокремлює 65 базових показників, тобто мінімально необхідну множину показників, які дозволяють проводити оцінювання тринадцяти базових практик безпеки. Ці базові практики є початковою точкою в процесі реалізації програми ЗБІ. Для підприємств чисельністю менш ніж 500 осіб (малі та середні підприємства) визначено п'ять фундаментальних практик безпеки, які спираються на множину із 40 показників безпеки інформації.

Відмітною особливістю наведеної таксономії показників безпеки інформації є те, що усі показники кількісні та представлені у вигляді процентів. Під час розробки системи практик робоча група спиралась на розробки NIST [8] та систему оцінювання корпоративної інформаційної безпеки ISG.

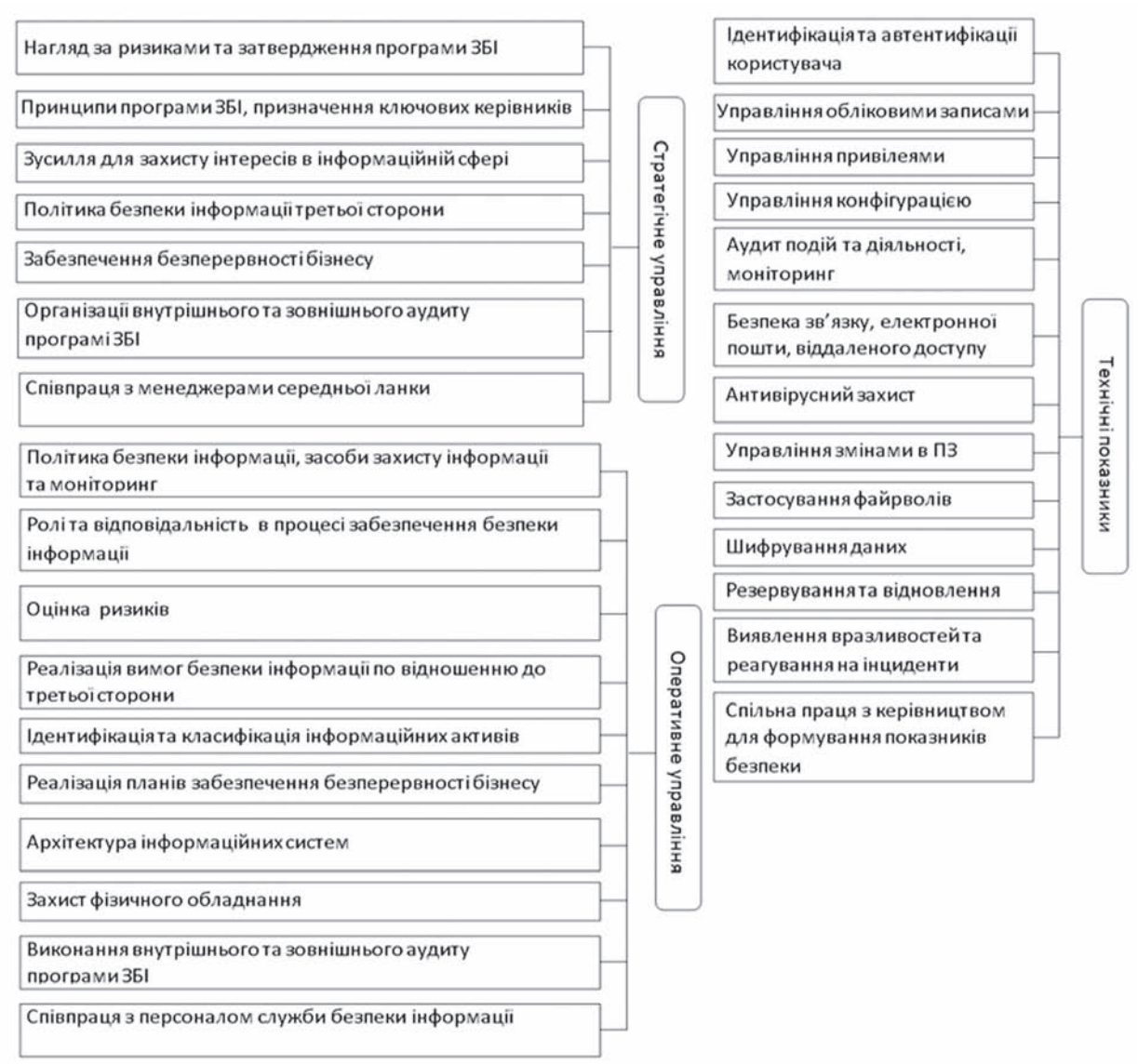

Рис. 5. Таксономія показників безпеки інформації CISWG

5. ТАКСОНОМИЯ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ ERKAN KAHRAMAN

Таксономія показників безпеки Erkan Kahraman (Стокгольмський університет) становить собою академічну розробку, запропоновану та створену автором у 2004 році [9]. Автор поставив перед собою мету розробити зручний інструмент, здатний підвищити ефективність управління безпекою, виконання аналізу ризиків, прийняття стратегічних рішень у контексті забезпечення безпеки інформації. Головним принципом, який було покладено автором в основу таксономії, є необхідність показників піддаватись кількісному обчисленню (наприклад, проценти, абсолютне число, відносне число). Показники також повинні легко визначатися та відзначатися певною гнучкістю під час вимірювань. Автор поставив перед собою наступні питання:

• Чи можливе вимірювання інформаційної безпеки підприємства взагалі?

• Якому рівню інформаційної безпеки відповідають певні значення показників безпеки?

• Як змінюється рівень інформаційної безпеки підприємства з часом?

Особливу увагу автор приділяє питанням оцінювання виконання тієї чи іншої діяльності із захисту інформації (security performance), оцінювання результативності та ефективності процесу забезпечення безпеки інформації. Формулювання цілей та задач безпеки інформації на думку автора необхідно здійснювати у формі високорівневих вимог політик безпеки. Автор вводить Ключові Індикатори Виконання (Key Performance Indicators, KPI), до яких відносяться:

• ефективність та результативність політик безпеки;

• вплив рівня компетентності на дії співробітників;

• робасність мереж та систем;

• реагування на інциденти безпеки та безперервне функціонування;

• управління доступом.

Показники безпеки пропонується визначати на основі трьох методів: методом контрольного списку (експертна оцінка по шкалі «так» (0) або «ні» (1)); методом бальної експертної оцінки у довільних шкалах та методом розрахунку показника шляхом об'єктивних вимірювань (у вигляді процентів). Процедура оцінювання здійснюється шляхом відповіді на поставлені питання. Всього сформульовано 90 питань.

6. ТАКСОНОМИЯ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ NIST

У 2005 році було завершено роботу рекомендацій NIST SP 800-53A [10]. Цей нормативний документ закріплює таксономію показників безпеки, побудовану на базі класифікації заходів захисту NIST SP 800-53 [11] (рис. 7).

У цілому таксономія NIST складається з трьох груп показників безпеки, що у свою чергу об'єднують 17 класів показників, які характеризують різні сімейства заходів захисту інформації (на рис. 9. наведено назви сімейств та їхні ідентифікатори). Слід зазначити, що запропонована класифікація помітно корелює із такими міжнародними стандартами, як ISO/IEC 17799 [4], ISO/IEC 13335 [12], а також з іншими нормативними документами США у сфері інформаційної безпеки. Це дозволяє зробити наступний висновок: підходи, застосовані під час розробки таксономії NIST досить легко адаптувати та розповсюдити на вимоги міжнародних стандартів, і таким чином побудувати відповідні таксономії показників безпеки.

Окрім того, в таксономії показників безпеки NIST досить чітко визначено об'єкт оцінювання

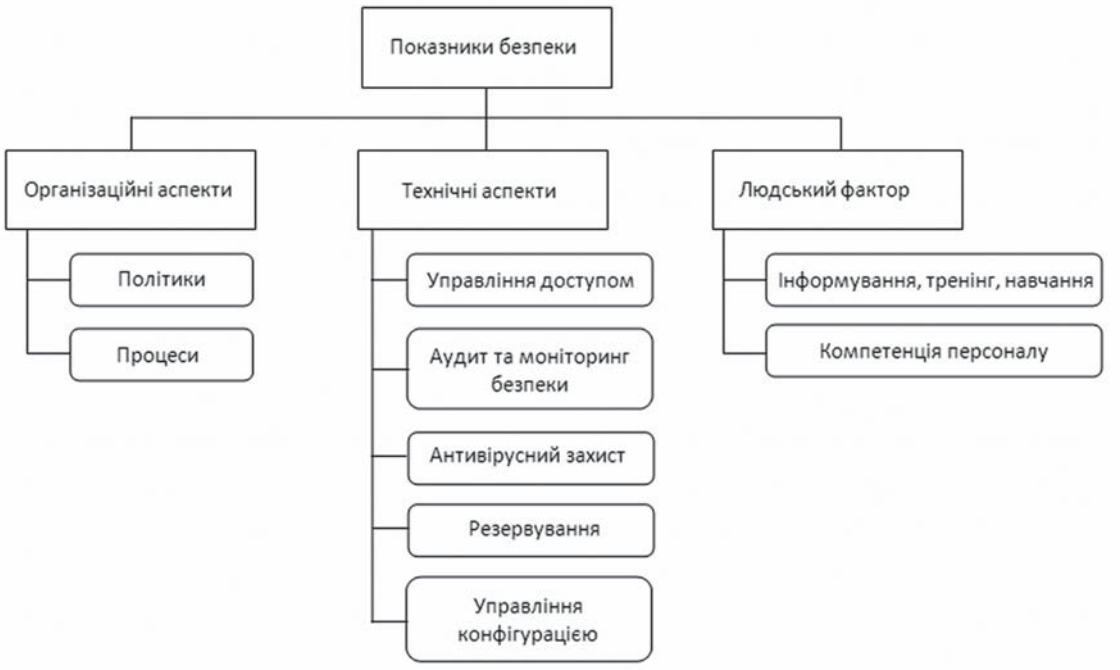

Рис. 6. Таксономія показників безпеки інформації Erkan Kahraman

– це заходи захисту, що реалізуються в інформаційних системах урядових закладах США. Використанню наведеної системи показників безпеки в урядових закладах приділяється велике практичне значення.

Зазначимо, що усі класи показників безпеки пропонується використовувати на організаційному рівні. Інакше кажучи, група технічних показників має мету оцінити рівень технічних засобів захисту інформації, що використовується на підприємстві. На відміну від таксономії Vaugh–Hennig–Siraj, група технічних показників NIST не призначена для оцінювання конкретного технічного об'єкту. Зазначимо також, що під час розробки таксономії NIST не було визначено критерії, у відповідності до яких здійснюється розбиття загальної множини показників на групи операційних, технічних або організаційних показників.

В рекомендаціях NIST SP 800-55 [8] у залежності від рівня виконання Програми ЗБІ, вводяться три типи показників безпеки:

• показники реалізації (виконання) заходів захисту інформації;

• показники результативності заходів;

• показники оцінки впливу заходів захисту на цільову функцію підприємства.

Показники різних типів можна використовувати одночасно. Проте, у залежності від рівня виконання програми ЗБІ виділяється і основний тип показників, що використовуються.

Якщо програма ЗБІ представлена у вигляді процедур (або процесів) і виконується у фокусі оцінювання реалізації елементів програми, тоді основними будуть показники виконання (наприклад, доля систем із затвердженими планами захисту). На першому та другому рівні виконання програми ЗБІ значення показників буде знаходитись у межах від 0 до 100%. На третьому рівні виконання програми припускається, що ці показники досягнуть максимального 100%-го рівня. Коли діяльність із захисту інформації стає систематичною, цілеспрямованою, керованою, а дані відносно її реалізації більш доступними та об'єктивними, основними показниками безпеки стають показники оцінювання результативності (наприклад, оперативність реагування на інциденти безпеки, своєчасність надавання послуг безпеки). Фокус уваги ЛПР зміщується з вирішень задач реалізації у бік вирішення задач забезпечення ефективності програми ЗБІ.

Показники впливу стають основними у разі повної інтеграції діяльності із захисту інформації у бізнес-процеси підприємства. Такі показники визначають, наприклад, кількість інцидентів безпеки за типами та їхню кореляцію з рівнем підготовки персоналу, або кількість втрачених клієнтів компанії через зниження репутації. Таким чином, на 4 та 5 рівнях виконання програми ЗБІ особливої ваги набувають показники ефективності і оцінювання корисності захисту інформації для підприємства.

7. ГОЛОВНІ ПРОБЛЕМИ РОЗРОБКИ ТА ІНТЕГРАЦІЇ ПОКАЗНИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сьогодні існують певні фактори, що перешкоджають широкому використанню та інтеграції показників безпеки:

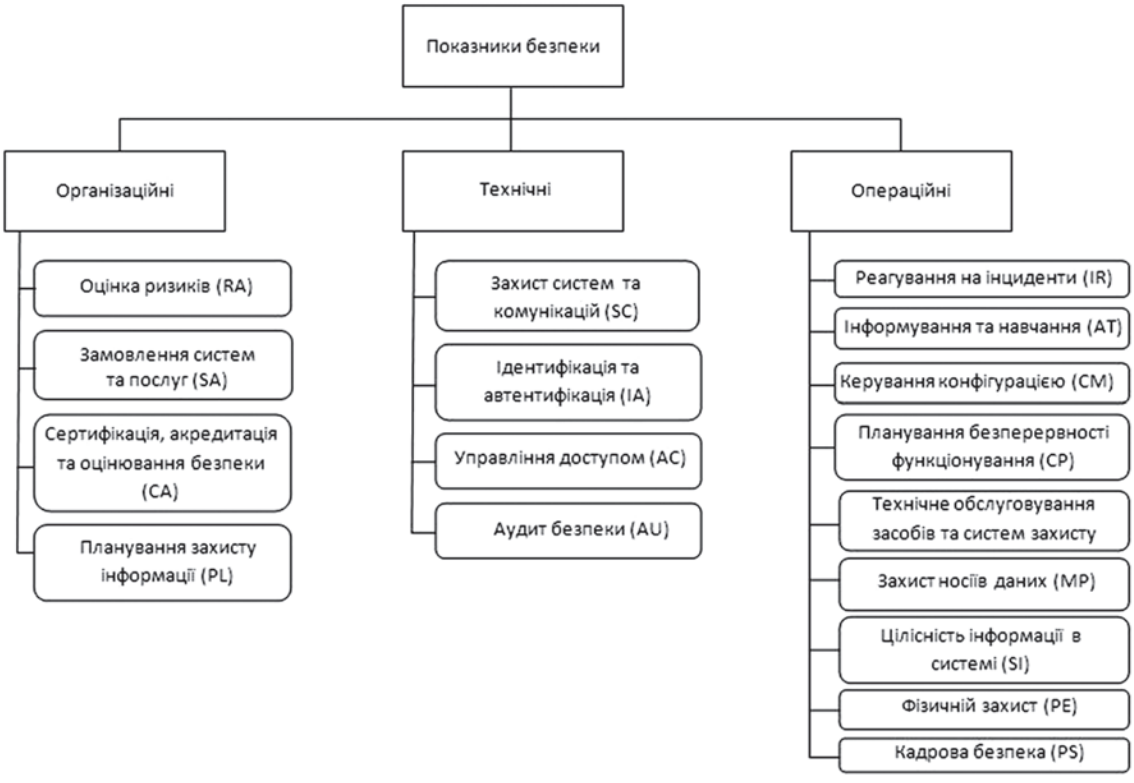

Рис. 7. Таксономія показників безпеки інформації NIST

• Неясність терміну «показник безпеки», "security metric", недостатня об'єктивність результатів процесу оцінювання;

• Певні труднощі в отриманні кількісних результатів оцінювання об'єктів інформаційної безпеки;

• Труднощі з оцінювання операційних показників безпеки;

• Сам по собі характер проблем інформаційної безпеки.

Оцінювання людського фактора в контексті інформаційної безпеки є важливою задачею, проте нетривіальною. Існує протиріччя між оцінюванням безпеки та захистом особистої інформації, тому досить зрозумілим є бажання не завдати шкоди особистим інтересам людини, діяльність якої буде підлягати оцінюванню. З цієї позиції важливими напрямками є оцінювання вмотивованості, лояльності, компетенції, знань та досвіду співробітників у сфері інформаційної безпеки. Виділимо основні проблеми, що стосуються різних аспектів безпеки інформації.

Проблеми та задачі в області поведінкового аспекту:

• Щоденне оцінювання діяльності із забезпечення безпеки інформації;

• Оцінювання рівня культури інформаційної безпеки на підприємстві;

• Оцінювання поведінки співробітників;

• Оцінювання процесів навчання співробітників у сфері інформаційної безпеки.

Проблеми розробки організаційних та операційних показників безпеки інформації:

• Якісне оцінювання рівня безпеки інформації;

• Внутрішній аудит;

• Досягнення оптимального рівня безпеки систем;

• Необхідність введення базового рівня безпеки інформації;

• Зручність використання показників безпеки;

• Автоматизація збору даних;

• Мінімізація кількості показників безпеки інформації;

• Інтеграція показників безпеки у бізнес-процеси підприємства.

Складності технічного характеру:

• Ведення та аналіз журналів контролю;

• Необхідність аналізу мереж;

• Технічні засоби, що дозволяють автоматизацію;

• Відстеження вірусів та їх локалізація в системах та мережах;

• Безумовна стійкість продуктів, процесів та робіт;

• Самонавчання.

ВИСНОВКИ

Проаналізувавши існуючі на сьогоднішній день таксономії показників безпеки інформації, можна дійти висновку, що взагалі існує три типи систем: таксономії, що містять виключно кількісні показники (CISWG); таксономії, що містять виключно якісні показники (OCTAVE); таксономії змішаного типу, що містять показники обох типів (NIST, Erkan Kahraman). Таким чином, усі існуючі на сьогоднішній день таксономії спираються на розділення усієї множини показників на три категорії: організаційні, операційні та технічні показники. Це говорить про те, що серед фахівців склався погляд, що усебічне оцінювання рівня безпеки інформації можна провести тільки враховуючи різних факторів та аспектів захисту інформації. Головний та спільний для цих таксономій недолік – це відсутність рекомендацій щодо розробки комплексних, інтегральних показників. Це є досить суттєвим недоліком, оскільки вище керівництво зацікавлене у інтегральних показниках безпеки в контексті прийняття стратегічних рішень.

Інша значна проблема стосується інтерпретації конкретних значень показників безпеки (які в свою чергу можуть бути представлені у різних формах). Наприклад, керівнику служби безпеки доповідають «коефіцієнт персоналу, що пройшов тренінг з безпеки, становить 0.62». Одразу ж виникає питання, достатньо цього значення чи ні. Таким чином, саме лінгвістична оцінка впливає на ЛПР як значущий сигнал та найкращим чином спонукає його до прийняття рішення.

Запропоновані фахівцями таксономії здебільшого вирішують проблему формування множини показників, що дозволять провести усебічне оцінювання стану безпеки інформації на підприємстві. Проте, в існуючій літературі відсутні будь-які методи або засоби узагальнення показників, тим самим отримуючи інтегральні оцінки стану безпеки інформації.

Література.

[1] Workshop on Information, Security System Scoring and Ranking (WISSSR, 2001) Information System Security Attribute Quantification or Ordering (Commonly but improperly known as Security Metrics) – Workshop Proceedings – May 21-23, 2001, Williamsburg, VA.

[2] *Rayford Vaughn Jr., Ronda Henning, Ambareen Siraj,* Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, 30th Hawaii International Conference on System Sciences, Big Island, Hawaii, January 7- 10, 2002.

[3] *Alberts C., Dorofee A.* Managing Information Security Risks "The OCTAVE Approach" Addison-Wesley Publishing 2003.

[4] NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996

[5] ISO/IEC 17799:2005 (BS 7799-1:2005) Information technology. Security techniques. Code of practice for information security management.

[6] *Seddigh N, P Pieda, A Matrawy, B Nandy, J Lambadaris, and A Hatfield.* 2004. "Current Trends and Advances in Information Assurance Metrics." Proceedings of the

Second Annual Conference on Privacy, Security and Trust (October 2004).

[7] Corporate Information Security Working Group (CISWG). November 17, 2004 (Revised January 10, 2005). Report of the Best Practices and Metrics Teams, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Government Reform Committee, United States House of Representatives.

[8] NIST SP 800-55, Security Metrics Guide for Information Technology Systems, July 2008.

[9] *Erkan Kahraman*. Evaluating it security performance with quantifiable metrics. Master's thesis, DSV SU/KTH, 2005.

[10] NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, July 2008.

[11] NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Aug. 2009.

[12] ISO/IEC 13335-1:2004 Information technology. Security techniques. Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management.

Надійшла до редколегії 7.06.2010.

Потій Олександр Володимирович, доктор техн. наук, доцент, начальник кафедри радіоелектронних систем пунктів управління повітряних сил Харківського університету повітряних сил ім. І. Кожедуба. Область наукових інтересів: проектування комплексних систем захисту інформації, криптографічних засобів захисту інформації; методи системного анализу процесів захисту інформації; методи оцінки безпеки об'єктів інформаційної діяльності.

Пилипенко Дмитрий Юрьевич, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: комплексные системы защиты информации, управление информационной безопасностью.

УДК 681.3.06

Анализ систем показателей безопасности информации / А.В. Потий, Д.Ю. Пилипенко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 435-443.

В работе проведен анализ существующих на сегодняшний день систем показателей безопасности информации. Данные системы или таксономии были рассмотрены в качестве инструмента, способного предоставить возможность комплексно охарактеризовать состояние безопасности информации на предприятии. Рассматривая показатели безопасности в данном контексте, были выделены их ключевые особенности, преимущества и недостатки.

Ключевые слова: показатель безопасности информации, программа обеспечения безопасности информации, таксономия показателей безопасности.

Ил. 07. Библиогр.: 12 назв.

UDC 681.3.06

Analysis of security metrics taxonomies / A.V. Potii, D.Yu. Pilipenko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 435-443.

The paper presents analysis of existing security metrics taxonomies. The security metrics taxonomies have been considered as an instrument, which allows comprehensive information security assessment within an organization. Analyzing the security metrics taxonomies in terms of information security evaluation, the most significant features, advantages and disadvantages have been defined.

Key words: security metrics, security program, security metrics taxonomy.

Fig. 07. Ref.: 12 items.