© Tsurkan V. Method of information security management system structure synthesizing // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 2, pp. 116-122.

DOI: 10.18372/2225-5036.26.14926

МЕТОД СИНТЕЗУВАННЯ СТРУКТУРИ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Василь Цуркан

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України

ЦУРКАН Василь Васильович, к.т.н., доцент

Рік та місце народження: 1982 рік, м. Харків, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут» (з 2016 року - Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського)», 2005 рік.
Посада: старший науковий співробітник з 2019 року.
Наукові інтереси: інформаційна безпека, кібербезпека, теорія ризику, системні дослідження.
Публікації: понад 100 наукових публікацій, серед них монографії, наукові статті.
E-mail: v.v.tsurkan@gmail.com.
Orcid ID: 0000-0003-1352-042X.

Анотація. *Розглянуто потреби, очікування та пов'язані з ними обмеження зацікавлених сторін як вхідні дані для специфікування вимог до систем управління інформаційною безпекою. Вони доповнюються встановленням внутрішніх і зовнішніх обставин, що впливають або можуть впливати на діяльність організацій. За специфікацією вимог визначається множина взаємопов'язаних функцій з внутрішніми та зовнішніми інтерфейсами. Кожна з них розкладається відповідно до структурних елементів систем управління інформаційною безпекою на функції підсистем, комплексів, компонентів. При цьому показується недостатність визначення структурних елементів і властивих їм функцій. Це обмежується необхідністю з'ясування сутності систем управління інформаційною безпекою з огляду на потреби, мету, процеси, структуру організацій. Тому вони розглядаються як сукупність підсистем, комплексів, компонентів, так і відношень між ними. Загалом цією сукупністю утворюється структура систем управління інформаційною безпекою. Для її представлення використовуються діаграми в графічній нотації SysML. За нею структурні елементи відображаються блоками як модульними одиницями. Тому системи управління інформаційною безпекою представляються деревом модульних одиниць. Характерні для них ознаки визначаються властивостями. Серед властивостей виокремлюються спеціальні класи – порти та обмеження. Їхнє використання дозволяє акцентувати на обмеженнях і особливостях взаємодії блоків між собою. Тоді як особливості такої взаємодії враховуються типами відношень. Тож методом синтезування структури систем управління інформаційною безпекою визначаються її структурні елементи (підсистеми, комплекси, компоненти) та відношення між ними. Завдяки цьому можливе встановлення властивостей даних систем стосовно конкретних варіантів розроблення і демонстрування вірогідних напрямів досягнення поставленої мети. Зокрема, збереження конфіденційності, цілісності та доступності інформації в організаціях шляхом оцінювання ризиків. Цим гарантується досягненість системами управління інформаційною безпекою запланованих результатів впровадження. Насамперед надання впевненості зацікавленим сторонам належного управління ризиками з прийнятним рівнем.*

Ключові слова: *блок, властивість, відношення, структурний елемент, структура, система управління інформаційною безпекою, діаграма структури, SysML.*

Вступ

Вхідними даними для розроблення систем управління інформаційною безпекою є потреби, очікування і пов'язані з ними обмеження з боку зацікавлених сторін. Вони доповнюються встановленням внутрішніх і зовнішніх обставин, що впливають або можуть впливати на діяльність організацій. На основі їхнього аналізування визначаються вимоги до систем управління інформаційною безпекою. Завдяки цьому встановлюються відповідності індивідуальним, груповим характеристикам, систематизуються, виявляються відношення між ними і, як наслідок, специфікуються вимоги. За такою специфікацією розробляється функціональна архітектура систем управління інформаційною безпекою. Це досягається визначенням множини взаємопов'язаних функцій шляхом їх функціонального аналізування. Кожна з них характеризується наявністю внутрішніх і зовнішніх інтерфейсів. Такі інтерфейси виникають унаслідок взаємодії функцій між собою. Відповідно до структурних елементів систем управління інформаційною безпекою вони розкладаються на функції. Так встановлюється послідовність виконання функцій системами управління інформаційною безпекою на рівнях їхніх структурних елементів [1-3].

Однак, при розробленні систем управління інформаційною безпекою недостатньо визначити структурні елементи та властиві їм функції. Це пов'язано з необхідністю з'ясування сутності таких систем з огляду на потреби, мету, процеси, структуру організацій. Тому вони представляються як сукупність підсистем, комплексів, компонентів, так і відношень між ними. Таке представлення тлумачиться

як структура. Нею визначаються властивості систем управління інформаційною безпекою стосовно конкретних варіантів розроблення. Як наслідок, демонструються вірогідні напрями досягнення поставленої мети – збереження конфіденційності, цілісності та доступності інформації в організаціях шляхом оцінювання ризиків. Цим гарантується досягненість системами управління інформаційною безпекою запланованих результатів впровадження. Насамперед надання впевненості зацікавленим сторонам належного управління ризиками з прийнятним рівнем. Тому синтезування структури систем управління інформаційною безпекою є актуальним завданням [1, 4, 5].

Аналіз існуючих досліджень

Розроблення систем управління інформаційною безпекою регламентується вимогами та настановами, імплементованих в Україні, міжнародних стандартів ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003 [1]. Відповідно до їхніх положень дослідження і публікації орієнтовані на розкриття окремих аспектів, наприклад [6-12]. У [6] акцентується на складнощах усвідомлення і забезпечення відповідності міжнародному стандарту ISO/IEC 27001. Для їх подолання пропонується метод оцінювання ризиків ISMS-CORAS. Ним визначаються технічні прийоми та рекомендації встановлення відповідності систем управління інформаційною безпекою. Інженерне середовище даних систем розглянуто в [7]. Зокрема, оцінюється ефективність його використання для підтримання організацій при розробленні систем управління інформаційною безпекою за вимогами ISO/IEC 27001. Аспекти забезпечення неперервності діяльності організацій розглянуто в [8]. Зокрема, розроблено фреймворк системи управління інформаційною безпекою. Він використовується для оцінювання рівня зрілості організацій і надання рекомендацій з впровадження процесів забезпечення інформаційної безпеки та управління відповідно до вимог ISO/IEC 27001. Рольову структуру системи управління інформаційною безпекою наведено в [9]. Визначено ролі працівників організації (на прикладі патентного відомства) стосовно забезпечення цілісності та доступності її інформаційних активів (заявок на винаходи, патентів). Розроблення, впровадження, контролювання та вдосконалення системи управління інформаційною безпекою на основі моделі зрілості представляється у [10]. Досягнення бажаного її рівня здійснюється створенням плану вдосконалення. Вхідними даними для нього є результати оцінювання зрілості організації стосовно забезпечення інформаційної безпеки. Конфіденційність, цілісність, доступність, загрозу, вразливість виокремлено як первинні параметри системи управління інформаційною безпекою у [11]. Значення кожного з них встановлюються методом контрольних списків. Його використання дозволяє оцінити відповіді розпорядників інформаційних активів і більш ефективно обрати засоби забезпечення інформаційної безпеки. Завдання формування прийнятних варіантів організаційного складу та структури автоматизованої системи управління різнорідними засобами захисту інформації вирішено в [12].

Отже, за результатами аналізування останніх досліджень і публікацій з'ясовано їхню орієнтованість на встановлення відповідності систем управління інформаційною безпекою вимогам і настановам міжнародних стандартів, зокрема, ISO/IEC 27001. По-перше, визначенням технічних прийомів та рекомендації методом оцінювання ризиків ISMS-CORAS [6]. По-друге, розробленням і впровадженням систем управління інформаційною безпекою за рівнем зрілості [8, 10]. По-третє, визначенням ролей працівників організації стосовно забезпечення цілісності та доступності її інформаційних активів [9]. По-четверте, виокремленням і встановленням значень первинних параметрів систем управління інформаційною безпекою методом контрольних списків [11]. По-п'яте, формуванням і управлінням прийнятними варіантами різнорідних засобів захисту інформації [12]. Однак, поза увагою залишається аспект виокремлення структурних елементів (підсистем, комплексів, компонентів), відношень між ними. Для цього запропоновано використання діаграм структури в графічній нотації SysML [3].

Метою даної роботи є визначення структурних елементів, відношень між ними систем управління інформаційною безпекою методом синтезування їхньої структури.

Основна частина дослідження

Структурні елементи систем управління інформаційною безпекою у графічній нотації SysML відображаються блоками [3]. Блок тлумачиться як модульна одиниця структури (див. рис. 1) [13, 14], якою моделюються підсистеми, комплекси, компоненти. Наприклад [15, 16]: оцінювання ризику, оброблення ризику; ідентифікування ризику, визначення оцінок ризику; ідентифікування вірогідності (ймовірності) реалізації загроз, ідентифікування наслідків реалізації загроз. Тому системи управління інформаційною безпекою представляються деревом модульних одиниць. Таке представлення дозволяє враховувати потреби, мету, процеси та структуру організацій. Воно реалізується шляхом визначення типів блоків, типів відношень між ними та способів їх поєднання відповідно до мети розроблення систем управління інформаційною безпекою. Зокрема, забезпечення інформаційної безпеки з прийнятним рівнем ризику та, як наслідок, гарантування зацікавленим сторонам належності управління ним в організації.

Для досягнення даної мети блоком визначається або одна, або декілька функцій відповідно до їхньої архітектури [16]. Структурні ознаки даного визначення характеризуються властивостями. Ними представляються тип і вказуються значення блоків, частин або посилання на інші блоки. Серед властивостей виокремлюються спеціальні класи – порти та обмеження. Портами відображаються прийнятні типи відношень між структурними елементами систем управління інформаційною безпекою. Зокрема, деталізуються місця підключення зовнішніх сутностей до блоків та способи взаємодії між ними. Наприклад, до блоку "Аналізування ризику" зовнішньою сутністю є інший блок "Зіставлення (атестування) ризику". Межі використання властивостей встановлюються обмеженнями. Наприклад, для блоку "Зіставлення (атестування) ризику" задається умова прийнятності / неприйнятності оцінок ризику для прийняття рішення про необхідність його оброблення [3, 13, 15].

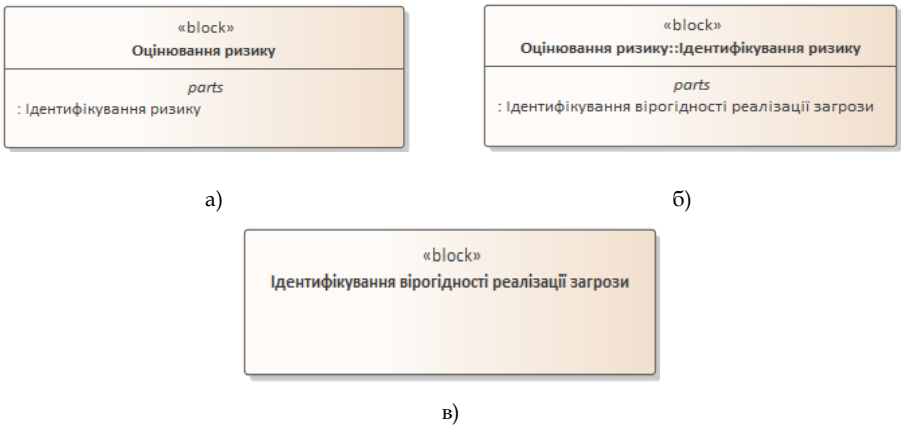

Рис. 1. Зображення структурних елементів систем управління інформаційною безпекою [3, 13, 17]:
а) підсистеми; б) комплексу; в) компоненту

Крім цього, для відображення структурних ознак блоків структури систем управління інформаційною безпекою у графічній нотації SysML виокремлюються три категорії властивостей [16]:

Частина – характеризує розкладання блоку на окремі складники. Взаємозв'язки між ними встановлюються за допомогою відношення композиціювання. Його використання орієнтоване на встановлення основних і додаткових властивостей блоку-частини в межах блоку-цілого. При цьому їхня кількість характеризується кратністю складника, що задається:

1) нижньою межею як мінімальною кількістю складників блоку-цілого. Задається нулем або будь-яким додатнім числом, наприклад: "0" – немає або "1" – один. Однак, при відображенні властивості "Частина" визначається тільки "0" або "1". Це обумовлено тим, що відношення композиціювання може встановлюватися тільки між двома блоками – цілим і його частиною. У цьому випадку встановлення "0" як нижньої межі означає існування блоку-частини без блоку цілого або його відсутність;

2) верхньою межею як максимальною кількістю складників блоку цілого. Задається або одиницею, або будь-яким додатнім числом, або "*" за великої кількості частин. При встановлені верхньої межі враховується умова, що вона рівна або більша за нижню. Тому верхня межа може визначатися лише "1". Це обумовлено існуванням блоку-частини тільки в межах одного блоку-цілого.

Властивість "Частина" відображається всередині блоку-цілого. Для цього відводиться окреме поле, що позначається словом "parts" (див., наприклад, рис. 1, б)). У такому полі кожному блоку-частині виділяється окремий запис. Зокрема, блок "Ідентифікування вірогідності реалізації загрози" є частиною блоку "Ідентифікування ризику". Тоді як останній є складником для цілого "Оцінювання ризику".

Посилання – характеризує включення до блоку інших блоків як його складників. Особливістю використання цієї властивості є можливість існування блоків-частин при знищенні цілого. Крім того воно застосовується для описання логічної ієрархії блоків структури систем управління інформаційною безпекою, що визначається блоками як елементами інших ієрархічних частин. За аналогією з властивістю "Частина" вказується всередині блоку-цілого в окремій секції. Для його позначення уживається слово "references" і виділяються окремі рядки для кожного посилання. Відношення між блоками задається типом "Агрегування" з визначенням кратності за аналогією з властивістю "Частина". Це означає, що нижня межа може дорівнювати "0" або "1", а верхня - "1". Наприклад, якщо розглядати як блок-ціле "Визначення оцінок ризику", то до нього можуть включатися блоки "Визначення якісних оцінок ризику", "Визначення кількісних оцінок ризику", "Визначення якісно-кількісних оцінок ризику". З огляду на характеризування взаємозв'язку між ними типу "Агрегування", кожна з цих частин може реалізовуватися як окремий структурний елемент, так і агрегуватися у межах блоку-цілого. Тоді його секція "references" визначатиметься трьома записами ": визначення якісних оцінок ризику", ": визначення кількісних оцінок ризику" ": визначення якісно-кількісних оцінок ризику".

Значення – використовуються для визначення характеристик структурних елементів систем управління інформаційною безпекою. До таких характеристик належать, наприклад: вірогідність (імовірність) реалізації загрози, наслідки реалізації загрози, оцінка ризику. Основою використання цієї властивості є встановлення діапазону її прийнятних значень при описанні блоку. Ці значення можуть бути типовими або, наприклад, визначатися законом розподілу ймовірності. Структура даних характеристик блоків описується типом значень на основі типів графічної нотації SysML або нових. Серед них виокремлюються:

1) примітивний тип – підтримуються скалярні значення, а саме: цілі, символьні, логічні та дійсні;

2) перелічуваний тип – визначається множина іменованих значень, що називаються літералами;

3) структурований тип – специфікується структура даних зі значеннями одного типу.

Оскільки типами представляються значення, то вони на відміну від блоків не характеризуються ідентичністю. Це означає, що їхня ідентичність визначається рівністю відповідних значень. Для задання властивостей "Значення" виділяється окрема секція блоку з ключовим словом "valueType". Тому при син-

тезуванні структури систем управління інформаційною безпекою важливо забезпечувати узгодженість типів значень характеристик її елементів.

Взаємозв'язок між структурними елементами систем управління інформаційною безпекою визначається відношеннями [16]. Встановленням їхнього типу враховуються його характер і особливості, наприклад [3, 16, 18, 19]: довільність, наслідуваність, узагальненість, структурність. Тож для визначення взаємозв'язку між структурними елементами систем управління інформаційною безпекою графічною нотацією SysML використовуються відношення асоціювання, узагальнення, агрегування, композиціювання [15, 16, 18, 19].

Асоціювання – тип відношення, яким визначається наявність взаємозв'язку між структурними елементами систем управління інформаційною безпекою (див., наприклад [3, 13, 17], рис. 2). Його використання вказує на довільність взаємодії або двох, або декількох блоків між собою. Рис. 2 демонструється приклад встановлення відношення типу "Асоціація" між блоками "Ідентифікування ризику" та "Визначення оцінок ризику". Цим ілюструється необхідність ідентифікування, зокрема, вірогідності (ймовірності) та наслідків реалізації загрози. Отримані результати комбінуються при визначенні оцінок ризику [20].

Рис. 2. Відношення асоціювання між блоками "Ідентифікування ризику" та "Визначення оцінок ризику"

Узагальнення – тип відношення, яким визначається взаємозв'язок між більш загальним ("батьком") і спеціалізованим стосовно нього ("нащадком") блоками (див., наприклад [3, 13, 17], рис. 3). З одного боку, це означає, що властивості батьківського блоку наслідуються блоками-нащадками. З іншого – ним можливе встановлення обмежень для блоків-нащадків при наслідуванні. Водночас останні можуть мати й додаткові властивості стосовно батьківського блоку. Направленість даного типу відношення дозволяє встановлювати ієрархічні взаємозв'язки тільки між двома структурними елементами систем управління інформаційною безпекою. Так, прикладом на рис. 3 демонструється наслідування блоком-нащадком "Визначення якісних оцінок ризику" властивостей батьківського блоку "Визначення оцінок". Насамперед атрибутів вірогідність (імовірність) реалізації загрози, наслідки реалізації загрози, оцінка ризику; операції визначення оцінок. Водночас блоку-нащадку властиві додаткові характеристики представлення результатів за порядковою шкалою [3]: низька, середня, висока.

Рис. 3. Відношення узагальнення між батьківським блоком "Визначення оцінок ризику" та блоком- нащадком "Визначення якісних оцінок ризику"

Агрегування – тип відношення, яким визначається взаємозв'язок між блоком та його складовими частинами (див., наприклад [3, 13, 17], рис. 4). Воно використовується для відображення системних зв'язків. Це означає, що структурні елементи систем управління інформаційною безпекою зіставляються як "ціле – частина". Тобто підсистеми ("ціле") можуть складатися з комплексів ("частина") або комплекс ("ціле") – з компонентів ("частина"). Їх використання дозволяє встановлювати відношення тільки між двома блоками. При цьому частини на відміну від відношення "Узагальнення" можуть мати відмінні властивості порівняно з цілим. Приклад встановлення взаємозв'язків "ціле-частина" показано на рис. 4. На ньому блок "Визначення оцінок ризику" зображується як "ціле". Тоді як його частинами є "Визначення якісних оцінок ризику" та "Визначення кількісних оцінок". Цим демонструються властивості блоку-цілого, якими враховується визначення оцінок залежно від обсягу даних про реалізації загроз і їхні наслідки для організації.

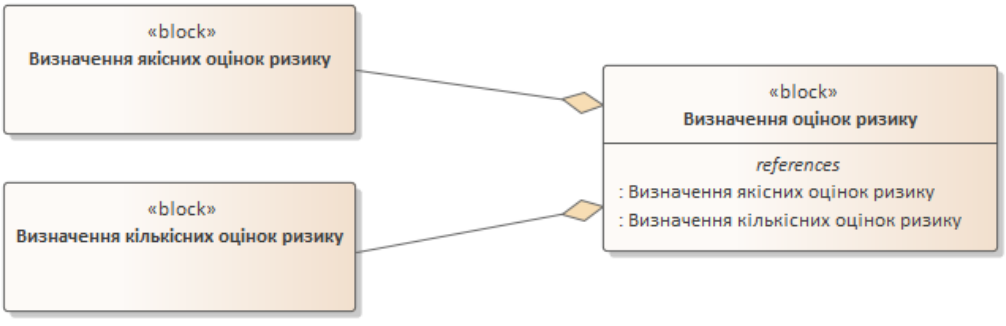

Рис. 4. Відношення агрегування між блоком-цілим "Визначення оцінок ризику" та блоками- частинами "Визначення якісних оцінок ризику", "Визначення кількісних оцінок ризику"

Композиціювання – тип відношення, яким визначається сильний взаємозв'язок між блоком-цілим та його складовими частинами (див., наприклад [3, 13, 17], рис. 5). Це означає, що видалення структурного елементу як цілого системи управління інформаційною безпекою призводить до знищення його складників. При цьому блок-частина може належати тільки одному композиту. Композиціювання розглядається як окремий випадок відношення "Агрегування". Його використання зображується на рис. 5. Як композит або блок-ціле показується "Аналізування ризику". Він складається з двох блоків-частин – "Ідентифікування ризику" та "Визначення оцінок ризику". Кожен з них може змінюватися до або після змінення цілого. Тому композит "Аналізування ризику" припиняє існувати внаслідок його видалення або окремих складників.

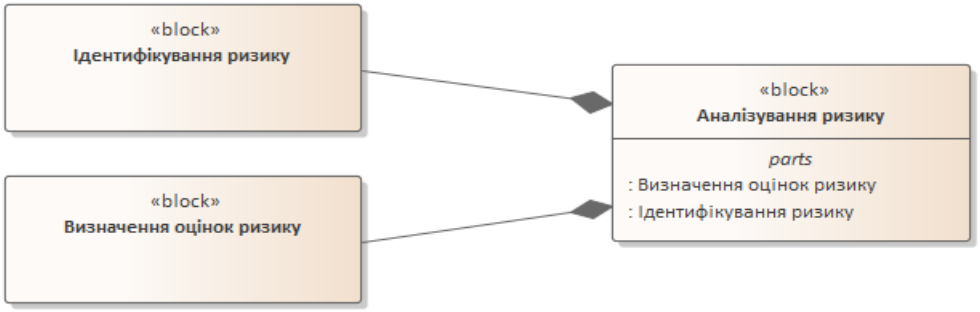

Рис. 5. Відношення композиціювання між блоками "Аналізування ризику" та блоками- частинами "Ідентифікування ризику ", "Визначення кількісних оцінок ризику"

Використання блоків і відношень між ними дозволяє синтезувати як структурні елементи систем управління інформаційною безпекою, так і встановити особливості їхнього представлення, взаємозв'язки блоків один з одним. Це узагальнюється завдяки використанню діаграм структури в графічній нотації SysML – визначення блоків і внутрішніх блоків [3]. Діаграмою визначення блоків відображається структура систем управління інформаційною безпекою зважаючи на її особливості (див., наприклад [13, 17], рис. 6). Тоді як для розкриття складових частин окремого структурного елементу використовується діаграма внутрішніх блоків.

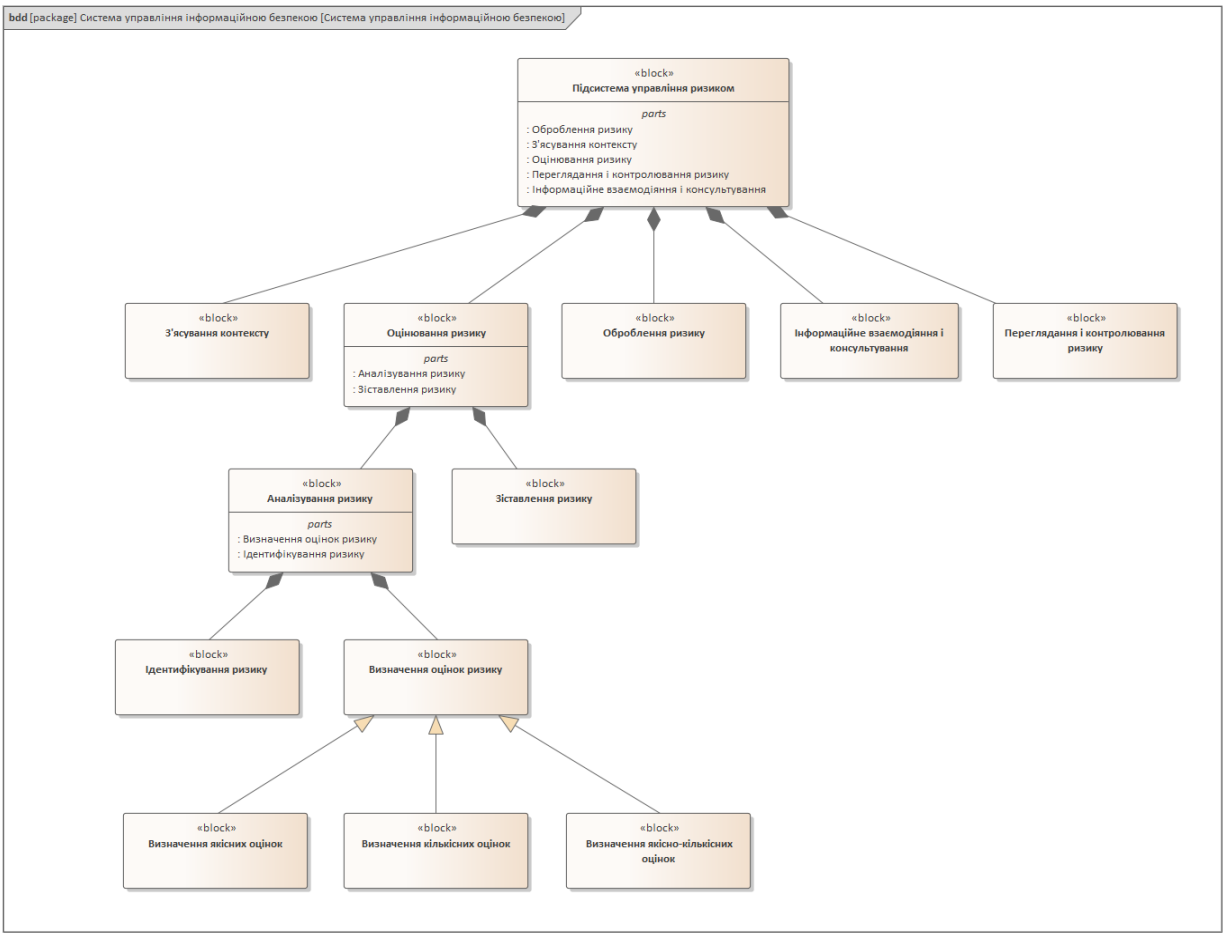

Рис. 6. Приклад синтезу структури систем управління інформаційною безпекою

Висновки

Отже, використання методу синтезування структури систем управління інформаційною безпекою дозволяє визначити її структурні елементи та відношення між ними. Для їхнього представлення застосовано діаграми структури в графічній нотації SysML. Воно реалізується шляхом визначення типів блоків, типів відношень між ними та способів їх поєднання. Завдяки цьому встановлюються властивості систем управління інформаційною безпекою стосовно конкретних варіантів розроблення і демонстрування вірогідних напрямів досягнення поставленої мети. Зокрема, збереження конфіденційності, цілісності та доступності інформації в організаціях шляхом оцінювання ризиків.

Література

[1]. *ISO/IEC 27001:2013, Information technology. Security techniques. Information security management systems. Requirements.* [Electronic resource]. URL: https://www.iso.org/standard/54534.html.

[2]. *ISO/IEC/IEEE 24748-4:2016. Systems and software engineering. Life cycle management. Part 4: Systems engineering planning*. [Electronic resource]. URL: https://www.iso.org/standard/56887.html.

[3]. В. Мохор, В. Цуркан, "Структурні елементи системи управління інформаційною безпекою", *Проблеми кібербезпеки інформаційно-телекомунікаційних систем*: *збірник матеріалів доповідей та тез міжнар. наук.-практ. конф., м. Київ, 12 черв. 2020 р.,* С. 332–334, 2020.

[4]. И. Прангишвили, *Системный подход и общесистемные закономерности. Серия "Системы и проблемы управления"*, Москва : СИНТЕГ, 2000, 528 с.

[5]. А. Антонов, *Системный анализ*, Москва: Высшая школа, 2004, 454 с.

[6]. K. Beckers, M. Heisel, B. Solhaug, K. Stolen, "ISMS-CORAS : A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System", *Engineering Secure Future Internet Services and Systems: Lecture Notes in Computer Science*, vol. 8431, Springer, Cham, pp. 315–344, 2014. DOI: 10.1007/978-3-319-07452-8_13.

[7]. A. Suhaimi, D. Bao, H. Chen, J. Cheng, "Usefulness of ISMEE for Supporting Organizations with ISMSs", *Computer Science and its Applications : Lecture Notes in Electrical Engineering*, vol. 330, Springer, Berlin, Heidelberg, pp. 1331-1336, 2015. DOI: 10.1007/978-3-662-45402-2_185.

[8]. A. Aginsa, I. Edward Matheus, W. Shalannanda, "Enhanced information security management system framework design using ISO 27001 and Zachman framework – A study case of XYZ company", *Wireless and Telematics (ICWT) : 2nd International Conference, Yogyakarta, 1–2 Aug. 2016, Yogyakarta*, pp. 62–66, 2016. DOI: 10.1109/ ICWT. 2016. 7870853.

[9]. В. Сиротюк, "Модели, методы и средства разработки и внедрения эффективной системы управления информационной безопасностью патентного ведомства", *Науковедение*, Т. 9, № 6, С. 1-19, 2017.

[10]. D. Proença, J. Borbinha, "Information Security Management Systems – A Maturity Model Based on ISO/IEC 27001", *Business Information Systems. BIS 2018 : Lecture Notes in Business Information Processing*, vol. 320, Springer, Cham, pp. 102-114, 2018. DOI: 10.1007/978-3-319-93931-5_8.

[11]. S. Mortazavi, F. Safi-Esfahani, A checklist based evaluation framework to measure risk of information security management systems", *International Journal of Information Technology,* Vol. 11, Iss. 3, pp. 517-534, 2019. DOI: 10.1007/s41870-019-00302-0.

[12]. В. Селифанов, Р. Мещеряков, "Методика формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления информационной безопасностью", *Моделирование, оптимизация информационные технологии*, Том 8, вып. 1, С. 1-13, 2020. DOI: 10.26102/2310-6018/2020.28.1.001.

[13]. *ISO/IEC 27005:2018, Information technology. Security techniques. Information security risk management.* [Electronic resource]. URL: https://www.iso.org/ru/standard/75281.html.

[14]. В. Цуркан, "Метод функціонального аналізування систем управління інформаційною безпекою", *Кібербезпека: освіта, наука, техніка*, Том 4, № 8, С. 192-201, 2020. DOI: 10.28925/2663-4023.2020.8.192201.

[15]. *OMG Systems Modeling Language (OMG SysML™).* [Electronic resource]. URL: https://sysml.org/res/docs/specs/OMGSysML-v1.6-19-11-01.pdf.

[16]. A. Moore, R. Steiner, *A Practical Guide to SysML. The Systems Modeling Language,* Waltham: Elsevier, 2015, 640 p.

[17]. *Model based systems engineering with Sparx Systems Enterprise Architect*. [Electronic resource]. URL: https://sparxsystems.com/resources/user-guides/.

[18]. А. Леоненков, *Самоучитель UML 2*, Санкт-Петербург : БХВ-Петербург, 2007, 576 с.

[19]. *Unified Modeling Language® (OMG UML®).* [Electronic resource]. URL: https://www.omg.org/spec/UML/2.5.1/PDF.

[20]. *ISO Guide 73:2009. Risk management. Vocabulary*. [Electronic resource]. URL: https://www.iso.org/standard/44651.html.

УДК 004[056.53+413.4]::303.732.4

Цуркан В.В. Метод синтезирования структуры систем управления информационной безопасностью

Аннотация. *Рассмотрены потребности, ожидания и связанные с ними ограничения причастных сторон как входящие данные для спецификации требований к системам управления информационной безопасностью. Они дополняются установлением внутренних и внешних обстоятельств, которые влияют или могут влиять на деятельность организаций. По спецификации требований определяется множество взаимосвязанных функций с внутренними и внешними интерфейсами. Каждая из них раскладывается в соответствии со структурными элементами систем управления информационной безопасностью на функции подсистем, комплексов, компонентов. При этом показывается недостаточность определения структурных элементов и свойственных им функций. Это ограничивается необходимостью выяснения сущности систем управления информационной безопасностью учитывая потребности, цель, процессы, структуру организации. Поэтому*

они рассматриваются как совокупность подсистем, комплексов, компонентов, так и отношений между ними. В общем этой совокупностью образуется структура систем управления информационной безопасностью. Для ее представления используются диаграммы в графической нотации SysML. За ней структурные элементы отображаются блоками как модульными единицами. Поэтому системы управления информационной безопасностью представляются деревом модульных единиц. Характерные для них признаки определяются свойствами. Среди свойств выделяются специальные классы – порты и ограничения. Ихние использование позволяет акцентировать на ограничениях и особенностях взаимодействия блоков между собой. Тогда как особенности такого взаимодействия учитываются типами отношений. Таким образом, методом синтезирования структуры систем управления информационной безопасностью определяются ее структурные элементы (подсистемы, комплексы, компоненты и отношения между ними. Благодаря этому возможно установление свойств данных систем относительно конкретных вариантов разработки и демонстрация возможных направлений достижения поставленной цели. В частности, сохранение конфиденциальности, целостности и доступности информации в организациях путем оценивания рисков. Этим гарантируется достигаемость системами управления информационной безопасностью запланированных результатов внедрения. Прежде всего представление уверенности заинтересованным сторонам надлежащего управления рисками с приемлемым уровнем.
Ключевые слова: *блок, свойство, отношение, структурный элемент, структура, система управления информационной безопасностью, диаграмма структуры, SysML.*

Tsurkan V. Method of information security management system structure synthesizing
Abstract. *The requirements, expectations, and related restrictions of interested parties are considered as input data for the specification of requirements for information security management systems. They are complemented with the establishment of internal and external factors that influence or can influence the activity of the organizations. According to the requirements specification, many interrelated functions with internal and external interfaces are defined. Each of them is decomposed according to the structural elements of information security management systems into the functions of subsystems, complexes, components. This shows the insufficiency of the definition of structural elements and their inherent functions. This is limited by the need to clarify the essence of information security management systems, taking into account the needs, goals, processes, structure of organizations. Therefore, they are considered as a set of subsystems, complexes, components, and relations between them. In general, this combination forms the structure of information security management systems. To represent it, diagrams in SysML graphic notation are used. Behind it, structural elements are reflected in blocks as modular units. Therefore, information security management systems are represented by a tree of modular units. Characteristics for them are determined by properties, among the properties stand out special classes - ports and restrictions. Their use allows to focus on the limitations and features of the interaction of blocks with each other. While the features of such interaction are taken into account by the types of relations. Therefore, by synthesizing the structure of information security management systems, its structural elements (subsystems, complexes, components) and the relationship between them are determined. Due to this, it is possible to set the properties of these systems regarding specific options for developing and demonstrating possible directions for achieving the goal. In particular, confidentiality, integrity and availability of information in organizations through risk assessment. This ensures that information security management systems achieve the planned implementation results. First of all, providing confidence to stakeholders to properly manage risks at an acceptable level.*
Keywords: *block, property, relationship, structural element, structure, information security management system, structure diagram, SysML.*

Цуркан Василь Васильович, кандидат технічних наук, доцент, старший науковий співробітник, Інститут проблем моделювання в енергетиці імені Г.Є. Пухова Національної академії наук України.
Цуркан Василий Васильевич, кандидат технических наук, доцент, старший научный сотрудник, Институт проблем моделирования в энергетике имени Г.Е. Пухова Национальной академии наук Украины.
Tsurkan Vasyl, candidate of technical sciences, associate professor, senior researcher, Pukhov Institute for Modeling in Energy Engineering of National Academy of Sciences of Ukraine.

Отримано *13 червня 2020 року*, затверджено редколегією *11 липня 2020 року*